MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

RTCA/DO-330解説書

平成25年2月
MHIエアロスペースシステムズ株式会社

- 1 -

【N/A】

目　次

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

1. DO-330とは
2. ツール資格計画プロセス
3. ツール開発ライフサイクル
4. ツール開発プロセス
5. ツールテストプロセス
6. ツール検証プロセス
7. ツール形態管理プロセス
8. ツール品質保証プロセス
9. ツール認証連絡調整プロセス
10. 追加の考慮事項

【N/A】

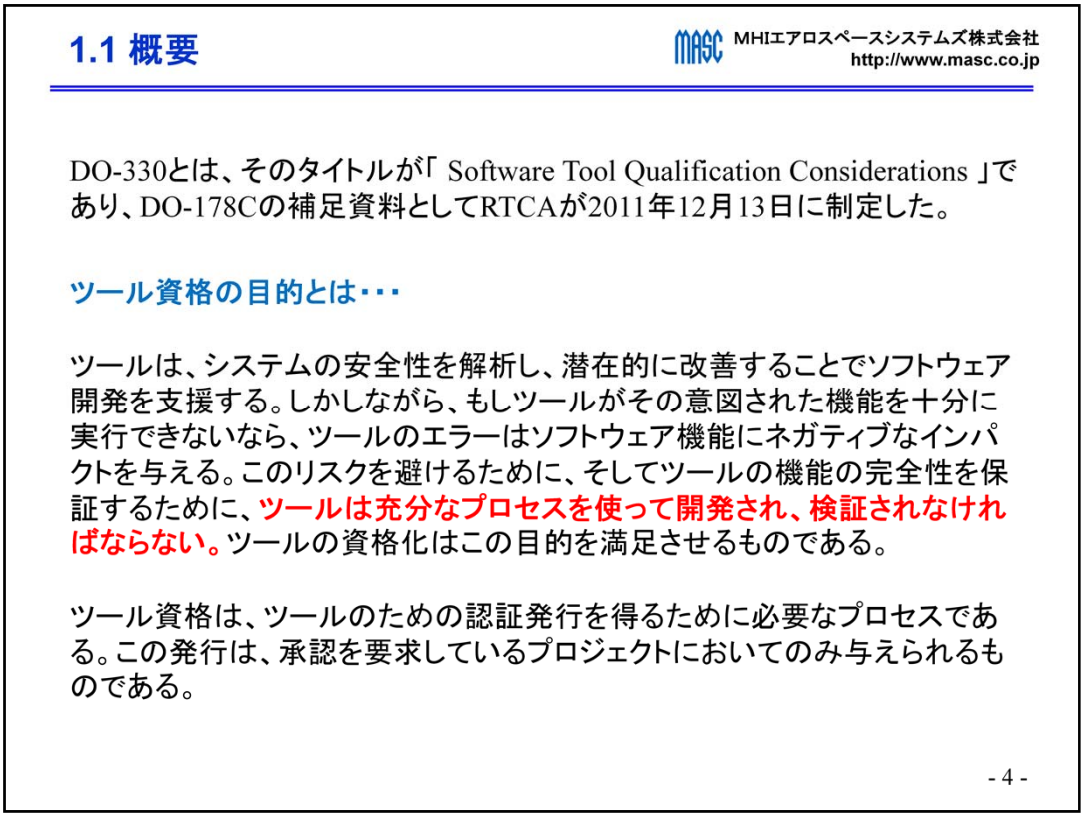
1. DO-330とは

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

1.1 概要
1.2 DO-178Cからの引用
1.3 ドキュメントオーバービュー
1.4 ツール・ライフサイクル・プロセス
1.5 ツール開発プロセス
1.6 インテグラルプロセス
1.7 各プロセスの関係
1.8 ツール資格データ
1.9 形態管理カテゴリ
1.10 各TQLで要求されるツール資格データ

- 3 -

【N/A】



【1.1-3.2】

《1.1》 Purpose

本書の目的はツール資格化のガイドラインを提供することである。加えて、説明資料をFAQsという形で提供している。

《1.1》

《1.2》 Scope

ソフトウェアツールは、複数のドメインで幅広く使用されている、例えば開発、検証、他のソフトウェアの管理における支援のために。

本書の中では、ツールはコンピュータプログラム、または機能的な部品であり、他のプログラム、そのデータ、文書の開発、変換、テスト、分析、製造、変更を手助けするために使用される。

例えば、自動コード生成、コンパイラ、テストツール、変更管理ツールなどである。

本書ではツールの資格化のためのプロセスと目的(Objectives)を説明している。

本書は以下の理由で作られた。

(a) ツールは、ツールを使用するソフトウェアと異なっており、独自のドメインを構成する。それゆえ、ツール開発者と利用者の両者にとって、ツール特有のガイドラインが必要となる。

(b) ツールは、しばしばソフトウェアを開発するためにツールを使用する者以外のチームによって開発される。これらのツール開発チームはしばしばソフトウェアのガイダンスのバックグラウンド(例えばDO-178CやDO-278Aと言ったガイドライン)がない。このツール特有の文書は、ツール開発チームに恩恵を与え、彼らが混乱し、誤解することを避ける手助けをする。

(c) 本書は航空そして地上のソフトウェアのためのガイダンスを提供する。それは他のドメイン（自動車、宇宙、システム、電子ハードウェア、航空データベース、安全性評価プロセスといった）に使われてもよい。

《1.2》 Scope

《1.3》How to Use This Document

ドメインもしくはプロジェクトが本書の使用を望む場合には、次のことを考慮しなければならない。

(a) 最大限の適用性と適応性を提供するために、5つのツール資格化レベル(TQLs)が定義されている。しかしながら、全てのレベルが全てのドメインに適用できるわけではない。各ドメインはそれらの特別な要求に従い、TQLsの適用性を決めなければならない。
特定のツールが資格化される必要があるかどうか、またそのレベルを決定するために、適切なドメイン特定の文書(例えばRTCA、SAE、EUROCAE文書など)を参照して下さい。例えば、Appendix Bには、DO-278Aドメインにおいて、地上ベースの通信、航法、監視、航空管制ソフトウェア向けに、どのようにツール資格Criteria、及び適切なTQLを決めるかその方法を示している。
しかしながら、各ドメインでは異なるCriteriaを使用してもよい。例えば、全てのTQLsを使用しなくてもよいし、使用されたTQLsにマップされる異なるツールCriteriaを持ってもよいし、本書の目的(Objectives)のいくつかを特定の適用性に当てはめてもよい。

(b) 本書を通して「ソフトウェアライフサイクル」、「ソフトウェアプロセス」、「ソフトウェア計画」、「ソフトウェア」といった言葉は、ツールが使用される製品のライフサイクル、プロセス、計画、ドメインと言う意味で使用される(すなわち、ソフトウェアドメインは一般的なドメインの代わりに使用される)。
他のドメインにおける「ソフトウェア」という言葉は、適切なドメインによって置き換えられてもよい、例えば「電子的なハードウェア」、「システム」、「航空データベース」、「航空ソフトウェア」など。

(c) 「認証機関」という言葉が、ツール資格化データの承認を管理している者を特定するための一般的な用語として使われている。
同様に、「認証」という言葉も、適切な組織によってツールを使用した製品の承認の意味として一般的に使われている。
「申請者」という言葉も、ソフトウェアの承認及び／またはツールの資格化を求める者を特定するために使用される。

(d) この文書のふさわしい意図、解釈、適用は、適切な認証機関の承認を得るために、適切な計画の中に含まれるべきである。

(e) ツールライフサイクルとソフトウェアライフサイクル間の協調は以下のソフトウェアライフサイクルデータの中で実施され、文書化されるべきである。
・ツールとその資格化の必要性を特定する計画。このデータは本書ではPSACと呼ばれている。
・資格化されるツールのステータスを含む、実施された全ての活動の総括とステータス。このデータはこの文書ではSASと呼ばれている。
・ツールとツール資格化データの識別を含む、ソフトウェア環境の形態索引。このデータはこの文書ではSECIと呼ばれている。
ドメインに関係なく、等価のデータが作成されることが期待される。

(f) 本書では、ツールは、そのアウトプットが検証されることなく、ソフトウェアライフサイクルプロセスを省略、削除、自動化するために使用されることを前提としている、そして、これらのプロセスは目的(Objectives)のセットの形で定義されている。それゆえ、ツールの認証発行はひとつもしくはいくつかの目的(Objectives)に関連している。ドメインに対するガイダンスが「プロセス」や「目的(Objectives)」の形で定義されていないということも可能である。この場合、認証発行の定義はドメインの専門用語に適合されるべきである。

(g) ツール資格のCriteriaと適用されるTQLを定義したガイダンスがないドメインにおいて、このドメインのプロジェクトは本書を使用することを提案してもよい。適用されるTQLとその合理性はそのプロジェクトのPSACかそれと等価な文書内に定義されるべきである。

(h) 本書の利用者は各TQLの目的(Objectives)の適用を決定するためにAnnex Aを参照するべきである。

《1.3》

《2.0》ツール資格の目的

ツールは、実施すべき活動を自動化することによって、及び、人的エラーを引き起こしやすい機能を予測通りに実施

することによって、システムの安全性を解析し、潜在的に改善することでソフトウェア開発を支援する。しかしながら、もしツールがその意図された機能を十分に実行できないなら、ツールのエラーはソフトウェア機能にネガティブなインパクトを与える。このリスクを避けるために、そしてツールの機能の完全性を保証するために、ツールは充分なプロセスを使って開発され、検証されなければならない。ツールの資格はこの目的を満足させるものである。

ツール資格は、ツールのための認証発行を得るために必要なプロセスである。この発行は、承認を要求しているプロジェクトにおいてのみ与えられるものである。

ツール資格プロセスの目的は、ツールの機能に信頼を得ることである。ツールの資格の努力は、ツールのエラーがシステムの安全性、及びソフトウェアライフサイクルプロセスにおけるツールの使用にもたらす潜在的なインパクトにより異なる。システムの安全性に影響を与えるツールエラーのリスクが高くなれば、ツール資格に要求される厳格さも高くなる。

ツール資格プロセスは、ツールの中のひとつもしくはそれ以上の機能、単一のツール、ツールの集まりに適用されてもよい(11.1 複数機能のツールにおける追加情報を参照)。

資格化の努力の間、全ての資格化されたツールの機能のアウトプットは、本書の目的(Objectives)を使って正しさを示さなければならない。そのアウトプットが予想の範囲内で変化するツールに対しては、その変化がアウトプットの意図した使用に不都合な影響を与えないこと、及びアウトプットの正確性が実証されることを示さなければならない。しかしながら、そのアウトプットがソフトウェアの一部となり、それゆえエラーを内在させることができるツールにとっては、資格されたツールの機能が、同じ環境で操作されたとき同じインプットに対して同じアウトプットを作り出すことを実証しなければならない。

《2.0》

《3.1》 資格レベル

ツールに要求される資格レベルは、ツールの使用とソフトウェアライフサイクルプロセスにおけるその潜在的なインパクトに基づく。本書では、5つのツール資格レベル(TQL-1からTQL-5)を特定する。ソフトウェアライフサイクルプロセスにおけるツールの潜在的なインパクトが増えると、TQLの厳密さは、システム安全性における潜在的なインパクトにより増加する。どのレベルがツール資格に割り当てられるかの決定は、ドメインに関連したガイダンス(例えばDO-178Cの12.2章)の中で定義されたように、ソフトウェアライフサイクルプロセス内でのツールの使用の評価により決定される。

資格の厳格さのレベルは資格レベルにより変わる。TQL-1は最も厳格なレベルであり、よく定義され実行されたツールの開発、検証、インテグラルプロセス(検証の高度な独立性とともに)を要求する。残りのレベルは、厳格さの減少した量を要求する。TQL-5は最も少ない厳格さの資格レベルである。AnnexAに各TQLに適用される目的(Objectives)を定義する。

《3.1》

《3.2》 資格のステークホルダー

ツールの資格化は通常は、複数のステークホルダーを伴う。多くのプロジェクトでは、それはツール利用者とツール開発者の両方である。ツール利用者は通常、使用するツールを特定し、ソフトウェアプロセスにおけるそのインパクトを評価し、そのツールが使用されるソフトウェアプロセスの範囲内でツールの使用に取り組み、ソフトウェア承認の中でツールの資格化を実施する。ツール開発者は通常、ツールの開発、検証、インテグラルプロセスのプロセスを記述し、ツール操作要求(TOR)に表現されたユーザ要求に準拠して、ツールの開発に取り組む。

上に示した典型的なステークフォルダと役割は変化してもよい。加えて、追加のステークフォルダを特定してもよい(例えば、ツールインテグレータやツール検証者)。計画文書、PSACや、またはツール資格計画(TQP)(適用されるなら)は、ツール資格化努力に対するステークフォルダとその役割、各ステークフォルダの責任を特定しなければならない。申請者は、最終的に、全てのツール資格の目的(Objectives)が満足することを保証する責任がある。

《3.2》

1.2 DO-178Cからの引用 (1/3)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

1.2.1 概要

(1) ツールによりDO-178Cのプロセスが省略、削除、自動化される場合、ツールの資格化が必要である。ただし、ツールのアウトプットがソフトウェア検証プロセスにより検証されるのであればその限りでない。
(2) 複数の機能を持つツールの場合、機能間の保護が立証できれば、使用する機能のみを資格化すればよい。
(3) ツール資格はシステム単位に実施しなければならず、あるシステムで既に資格化されているツールを他のシステムで使用する場合も再資格化が必要である。

- 5 -

【DO-178C 12.2.1】

《DO-178C 12.2.1》 Determining if Tool Qualification is Needed

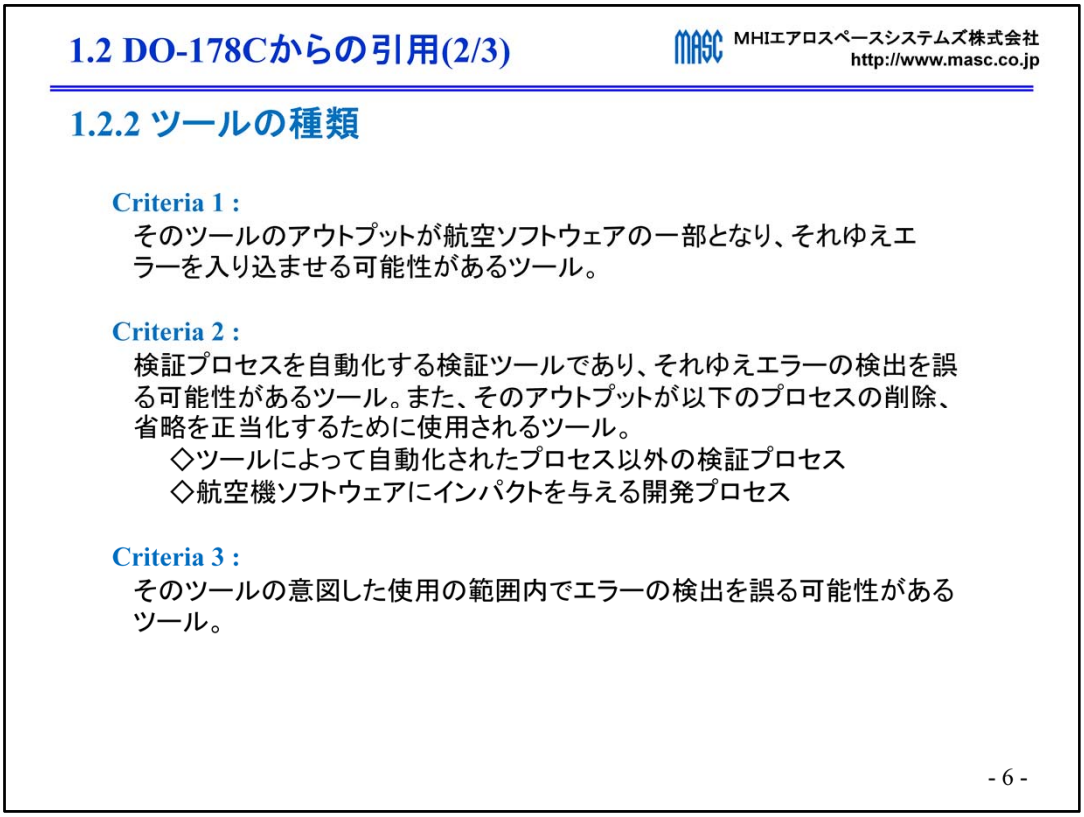
ツールの資格化は、そのアウトプットが6章(ソフトウェア検証プロセス)に規定された通りに検証された場合を除いて、ソフトウェアツールを使用することによって、DO-178Cのプロセスが省略、削除、自動化される場合必要となる。

ツール資格プロセスの目的は、省略、削除、自動化されたプロセスの信頼性と少なくとも等価の信頼性をツールが提供していることを保証するものである。

ツール資格プロセスは単体のツール、ツールの集まり、ツール内のひとつもしくはそれ以上の機能に適用してもよい。
複数の機能を持つツールに対しては、ツールの機能の保護が立証できれば、ソフトウェアライフサイクルプロセスを省略、削除、自動化するために(しかもそのアウトプットが検証されない)使用される機能のみを資格化する必要がある。
ここで保護とは、ツールの機能が他のツールの機能に意図しないインパクトを与えないことを保証する機構を使用することである。

ツールは、そのシステムのPSACにおいてツールを使用することが明言されたシステムでの使用においてのみ資格化される。あるシステムにおいて以前に資格化されたツールを他のシステムで使用する場合は、他のシステムの中で再資格化されなければならない。

《DO-178C 12.2.1》



【DO-178C 12.2.2】

1.2.2 ツールの種類

DO-178Bでは開発ツールと検証ツールの2種類だったのに対して3種類に分類している。

Criteria1は、コンパイラやコード自動生成ツールなどがそれに分類される。ただし、多くの場合「ツールのアウトプットがソフトウェア検証プロセスにより検証されるのであればツール資格の必要はない」に該当するのではないか。

ただし、コード自動生成ツールであったとしても、低レベル要求とソースコード間のトレーサビリティ(Table A-5 5. Source Code is traceable to low-level requirement)のプロセスを自動化、省略することを目的として使用するのであればCriteria2に分類されると思われる。

一方、検証ツールとしてテストツールやトレーサビリティの検証ツールなどがあるが、Criteria2か3のどちらに分類されるか判断は難しいところである。
計画の段階で使用するツールに関してどれに分類するべきかを認証機関と調整する必要がある。

《DO-178C 12.2.2》 Determining the Tool Qualification Level(ツール資格レベルの決定)

ツールの資格化が必要な場合、ツール資格レベル(TQL)を決めるために、ソフトウェアライフサイクルプロセスにおけるツール使用のインパクトが評価されるべきである。
ツールのインパクトを決めるために以下の評価基準(criteria)が使用されるべきである。

(a) Criteria 1
そのツールのアウトプットが航空ソフトウェアの一部となり、それゆえエラーを入り込ませる可能性があるツール。

(b) Criteria 2
検証プロセスを自動化する検証ツールであり、それゆえエラーの検出を誤る可能性があるツール。また、そのアウトプットが以下のプロセスの削除、省略を正当化するために使用されるツール。
1. ツールによって自動化されたプロセス以外の検証プロセス
2. 航空機ソフトウェアにインパクトを与える開発プロセス

(c) Criteria 3
そのツールの意図した使用の範囲内でエラーの検出を誤る可能性があるツール。

ツールがDO-178Cのプロセスを省略、削除、自動化し、そのアウトプットが6章の規定により検証されない場合、表12-1に示すような適切なTQLがある。

ツール資格の5つのレベル(TQL-1からTQL-5)は、ツールの使用とソフトウェアライフサイクルプロセスに与えるその潜在的なインパクトに基づいて特定される。

TQL-1は最も厳格なレベルであり、TQL-5は最も厳格でないレベルである。

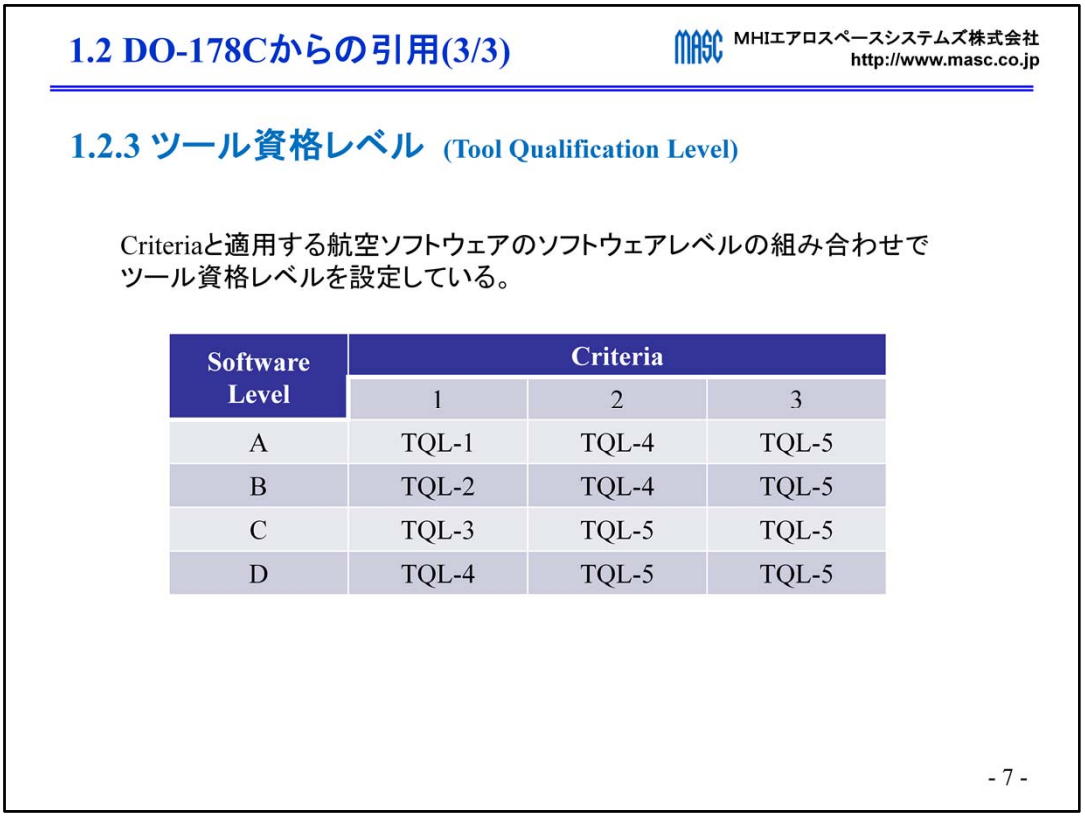
与えられたツールのインパクトを評価するとき、Criteriaは1から3へ順番に考慮されるべきである。

ツール資格レベル(TQL)は、可能な限り早い段階で認証機関と調整されるべきである。

表12-1 ツール資格レベルの決定

Software Level	Criteria 1	2	3
A	TQL-1	TQL-4	TQL-5
B	TQL-2	TQL-4	TQL-5
C	TQL-3	TQL-5	TQL-5
D	TQL-4	TQL-5	TQL-5

《DO-178C 12.2.2》



1.2 DO-178Cからの引用(3/3)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

1.2.3 ツール資格レベル (Tool Qualification Level)

Criteriaと適用する航空ソフトウェアのソフトウェアレベルの組み合わせで
ツール資格レベルを設定している。

Software Level	Criteria		
	1	2	3
A	TQL-1	TQL-4	TQL-5
B	TQL-2	TQL-4	TQL-5
C	TQL-3	TQL-5	TQL-5
D	TQL-4	TQL-5	TQL-5

- 7 -

【12.2.2】

1.2.3 ツール資格レベル(Tool Qualification Level)

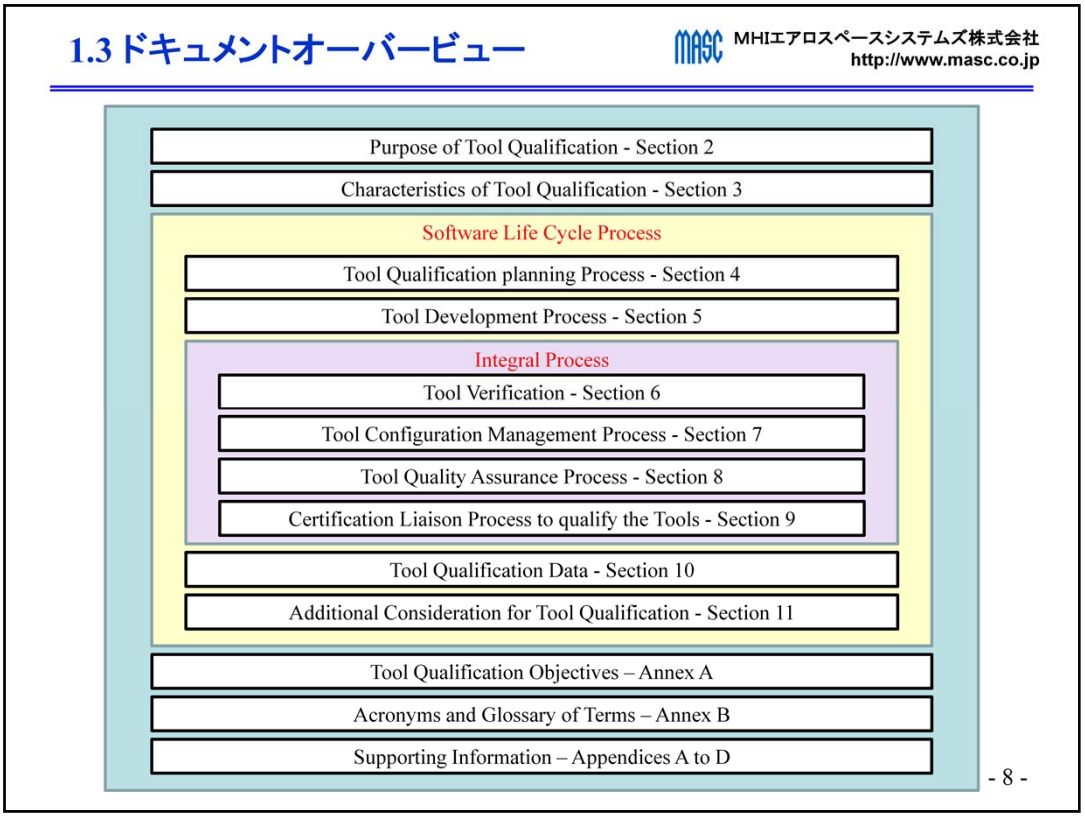
ツール資格レベルとしてTQL-1からTQL-5までの5段階が設定されている。
TQL-1が一番厳しいレベルであり、TQL-5が一番緩いレベルである。

プロジェクトで使用するツールの資格化が必要となった場合は、できるだけ早い時期に認証機関(Certification Authority)とTQLについて調整しなければならない。

<TQLに要求されるObjectivesの数>　　()内は独立した組織が実行

	TQL-1	TQL-2	TQL-3	TQL-4	TQL-5
Table T-0 (Operational)	7(3)	7(3)	7	7	6
Table T-1 (Planning)	7	7	7	2	0
Table T-2 (Development)	8	8	8	5	0
Table T-3 (Verification(Requirements))	9(6)	9(6)	9	8	0
Table T-4 (Verification(Design))	11(7)	11(3)	9	1	0
Table T-5 (Verification(Code & Integration))	7(3)	7(1)	6	0	0
Table T-6 (Testing)	4(2)	4(1)	4	2	0

Table T-7 (Verification(Testing))	9(9)	7(3)	6	2	0
Table T-8 (Configuration Management)	5	5	5	5	2
Table T-9 (Quality Assurance)	5(5)	5(5)	5(5)	2(2)	2(2)
Table T-10 (Liaison)	4	4	4	4	4
Total	76(35)	74(22)	70(5)	38(2)	14(2)



【1.4】

ここでは、DO-330の文書としての全体像を示している。

1.4 ツール・ライフサイクル・プロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

DO-330では、ツールのプロセスとして3プロセスを定義している。

ツール資格計画プロセス
(Tool Qualification Planning Process)

ツール開発プロセス
(Tool Development Process)

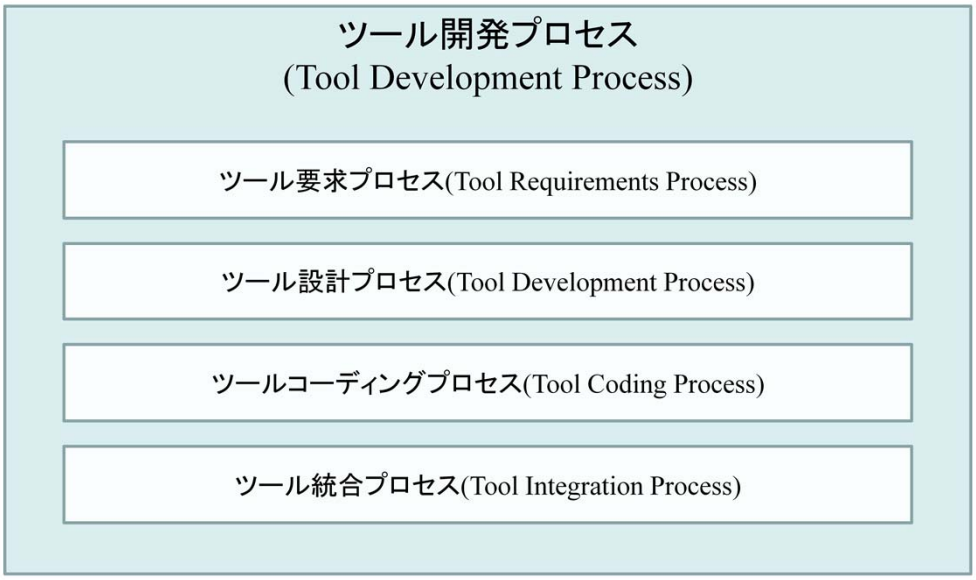
インテグラルプロセス
(Integral Processes)

- 9 -

【N/A】

1.5 ツール開発プロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp



- 10 -

【5】

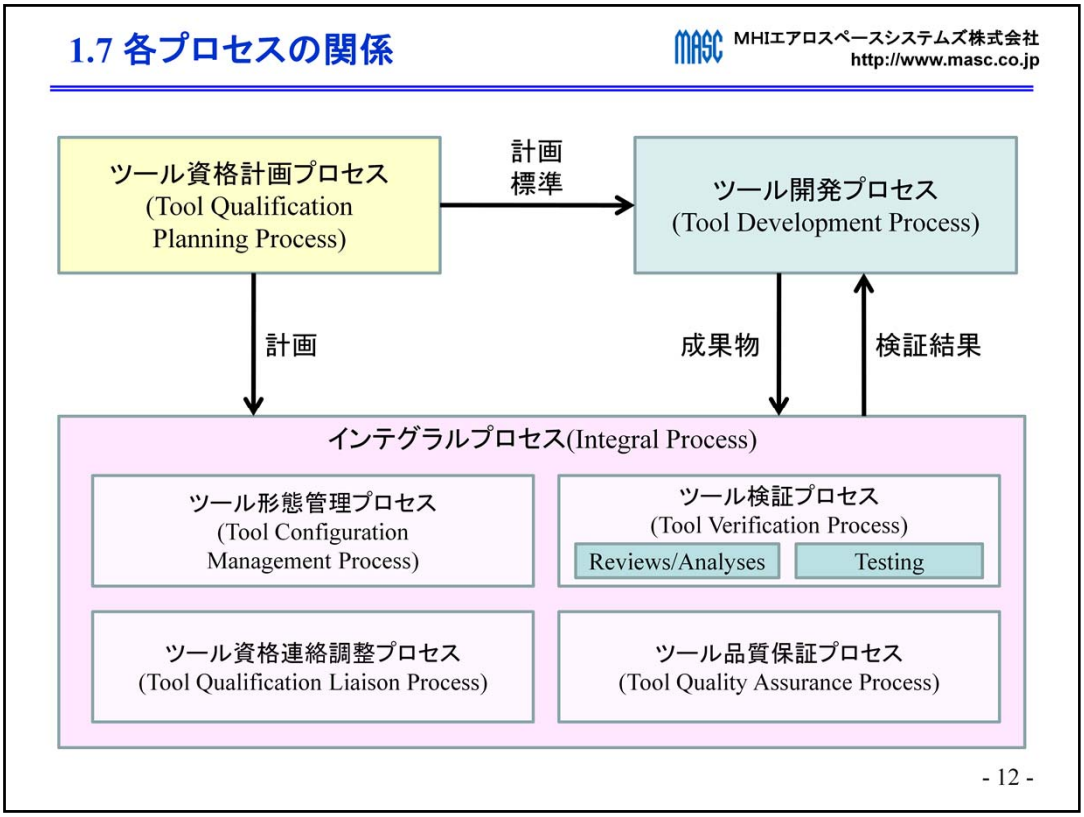
1.6 インテグラルプロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

インテグラルプロセス
(Integral Process)

- ツール検証プロセス(Tool Verification Process)
- ツール形態管理プロセス(Tool Configuration Management Process)
- ツール品質保証プロセス(Tool Quality Assurance Process)
- ツール資格連絡調整プロセス(Tool Qualification Liaison Process)

【N/A】



【N/A】

以上の3つのプロセスの関係を図に表した。

ツール資格計画プロセスで策定した計画、標準に従って、ツール開発プロセス、インテグラルプロセスは実行される。

ツール開発プロセスとインテグラルプロセスは併行して実行され、ツール開発プロセスの成果物（設計文書、ソースコード）がインテグラルプロセスに提供され、インテグラルプロセスの各プロセスで処理される。

特にツール検証プロセスの「Reviews/Analyses」と「Testing」は、ツール開発プロセスと密接に関連し、そのプロセスの成果物をレビュー／分析するとともに、実行可能オブジェクトコードのテストを実行する。

1.8 ツール資格データ (1/3)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

1.8.1 ツール資格連絡プロセスと他のインテグラルプロセスにおけるデータ

No	名　称	参照項番
1	PSAC内のツール固有情報(Tool-Specific Information in PSAC)	2.3-1
2	ツール資格計画(Tool Qualification Plan)	2.3-2
3	ツール開発計画(Tool Development Plan)	2.3-3
4	ツール検証計画(Tool Verification Plan)	2.3-4
5	ツール形態管理計画(Tool Configuration Management Plan)	2.3-5
6	ツール品質保証計画(Tool Quality Assurance Plan)	2.3-6
7	ツール要求標準(Tool Requirements Standards)	2.3-7
8	ツール設計標準(Tool Design Standards)	2.3-8
9	ツールコード標準(Tool Code Standards)	2.3-9
10	ツールライフサイクル環境形態索引 (Tool Life Cycle Environment Configuration Index)	7.5-1
11	ツール形態索引(Tool Configuration Index)	7.5-2
12	ツール不適合報告(Tool Problem Reports)	7.5-3
13	ツール形態管理記録(Tool Configuration Management Records)	7.5-4
14	ツール品質保証記録(Tool Quality Assurance Records)	8.4-1
15	ツール完了報告(Tool Accomplishment Summary)	9.3-3
16	ソフトウェア完了報告内のツール特有情報 (Tool-Specific Information in Software Accomplishment Summary)	9.3-1
17	ソフトウェアライフサイクル環境形態索引内のツール特有情報(Tool-Specific Information in Software Life Cycle Environment Configuration Index)	9.3-2

【10.1】

1.8 ツール資格データ (1/3)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

1.8.2 ツール開発プロセスと対応する検証活動の間に作られたツール資格データ

No	名　称	参照項番
1	ツール要求(Tool Requirements)	4.2.3-1
2	ツール設計記述(Tool Design Description)	4.3.3-1
3	ツールソースコード(Tool Source Code)	4.4.3-1
4	ツール実行可能オブジェクトコード(Tool Executable Object Code)	4.5.3-1
5	ツール検証ケース・手順(Tool Verification Cases and Procedures)	6.2-1
6	ツール検証結果(Tool Verification Results)	6.2-2
7	トレースデータ(Trace Data)	6.2-6

【10.2】

1.8 ツール資格データ (1/3)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

1.8.3 ツール運用要求プロセスとツール運用統合プロセス、および対応する検証/妥当性確認活動の間に作られたツール資格データ

No	名　称	参照項番
1	ツール運用要求(Tool Operational Requirements)	3.2.4-1
2	ツールインストール報告(Tool Installation Report)	6.2-3
3	ツール運用要求検証/妥当性確認ケース・手順 (Tool Operational Verification and Validation Cases and Procedures)	6.2-4
4	ツール運用要求検証/妥当性確認結果 (Tool Operational Verification and Validation Results)	6.2-5

【10.3】

1.9 形態管理カテゴリ

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

No	ツール形態管理プロセス活動	CC1	CC2
1	Configuration Identification	○	○
2	Baselines	○	
3	Traceability	○	○
4	Problem Reporting	○	
5	Change Control - integrity and identification	○	○
6	Change Control – tracking	○	
7	Change Review	○	
8	Configuration Status Accounting	○	
9	Retrieval	○	○
10	Protection against Unauthorized Changes	○	○
11	Media Selection, Refreshing, Duplication	○	
12	Release	○	
13	Data Retention	○	○

- 16 -

【7.3】

DO-178Cにおける形態管理と同様に、DO-330ではツール資格データの形態管理の方法を厳密に定義している。

詳細は6. ツール形態管理プロセスで説明するが、今後の説明の中で「形態管理カテゴリ」が随所に出てくるのでここで簡単に説明しておく。

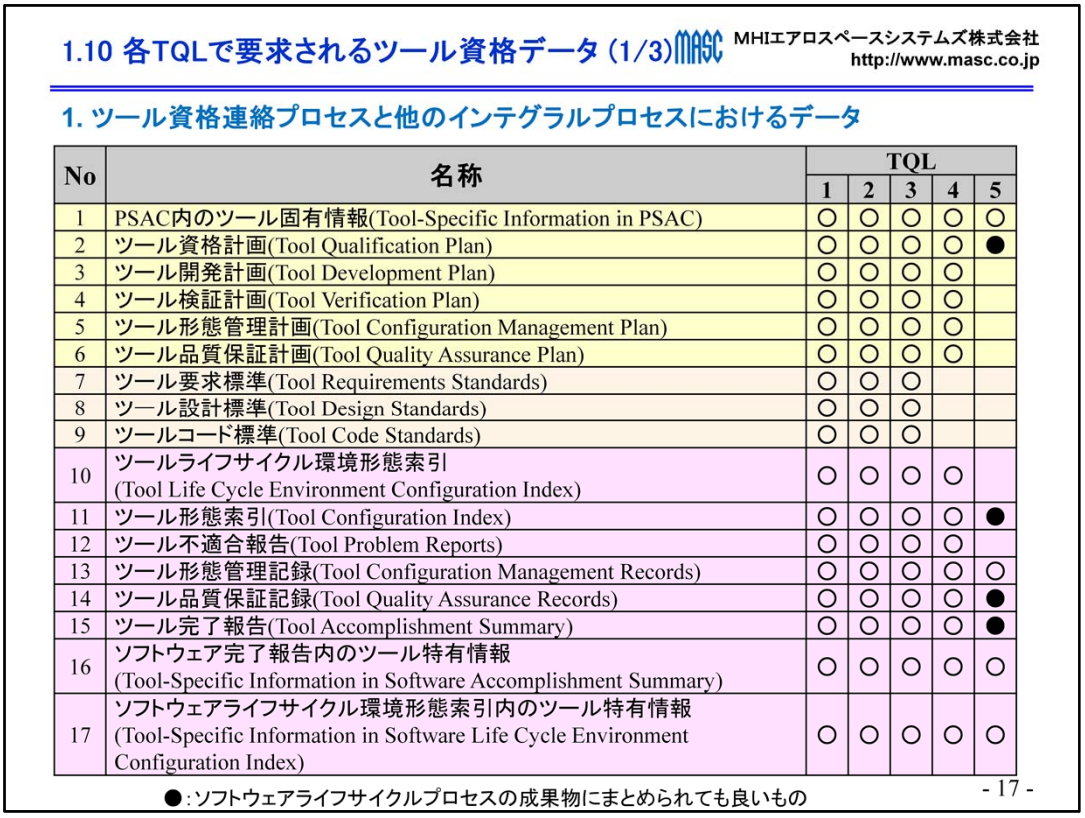
この表はツール形態管理プロセスで定義された13の形態管理項目を示している。

CC1は「Control Category 1」、CC2は「Control Category 2」の略である。

本資料では、「Control Category」を「形態管理カテゴリ」と訳している。

DO-330では、TQL(1～5)に応じてツール資格データの形態管理のレベル(CC1、CC2)を定めている。

CC1が指定されると13項目の全ての形態管理項目を実施する必要がある。CC2が指定された場合は、表で○のついた項目だけを最低限実施すればよい。



1.10 各TQLで要求されるツール資格データ (1/3)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

1. ツール資格連絡プロセスと他のインテグラルプロセスにおけるデータ

No	名称	TQL				
		1	2	3	4	5
1	PSAC内のツール固有情報(Tool-Specific Information in PSAC)	○	○	○	○	○
2	ツール資格計画(Tool Qualification Plan)	○	○	○	○	●
3	ツール開発計画(Tool Development Plan)	○	○	○	○	
4	ツール検証計画(Tool Verification Plan)	○	○	○	○	
5	ツール形態管理計画(Tool Configuration Management Plan)	○	○	○	○	
6	ツール品質保証計画(Tool Quality Assurance Plan)	○	○	○	○	
7	ツール要求標準(Tool Requirements Standards)	○	○	○		
8	ツール設計標準(Tool Design Standards)	○	○	○		
9	ツールコード標準(Tool Code Standards)	○	○	○		
10	ツールライフサイクル環境形態索引 (Tool Life Cycle Environment Configuration Index)	○	○	○	○	
11	ツール形態索引(Tool Configuration Index)	○	○	○	○	●
12	ツール不適合報告(Tool Problem Reports)	○	○	○	○	
13	ツール形態管理記録(Tool Configuration Management Records)	○	○	○	○	○
14	ツール品質保証記録(Tool Quality Assurance Records)	○	○	○	○	●
15	ツール完了報告(Tool Accomplishment Summary)	○	○	○	○	●
16	ソフトウェア完了報告内のツール特有情報 (Tool-Specific Information in Software Accomplishment Summary)	○	○	○	○	○
17	ソフトウェアライフサイクル環境形態索引内のツール特有情報 (Tool-Specific Information in Software Life Cycle Environment Configuration Index)	○	○	○	○	○

●:ソフトウェアライフサイクルプロセスの成果物にまとめられても良いもの

- 17 -

各TQLで要求されるツール資格データ(Tool Qualification Data)を示す。
○がついている項目が、そのTQLで開発しなければならないツール資格データである。

TQL-5の場合、成果物の一部(TQP, TCI, ツール品質保証記録, TAS)はソフトウェアライフサイクルプロセスの成果物にまとめられても良い。その項目を●で示した。

1.10 各TQLで要求されるツール資格データ (2/3)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

2. ツール開発プロセスと対応する検証活動の間に作られたツール資格データ

No	名称	TQL				
		1	2	3	4	5
1	ツール要求(Tool Requirements)	○	○	○	○	
2	ツール設計記述(Tool Design Description)	○	○	○	○	
3	ツールソースコード(Tool Source Code)	○	○	○		
4	ツール実行可能オブジェクトコード(Tool Executable Object Code)	○	○	○	○	○
5	ツール検証ケース・手順(Tool Verification Cases and Procedures)	○	○	○	○	
6	ツール検証結果(Tool Verification Results)	○	○	○	○	
7	トレースデータ(Trace Data)	○	○	○	○	

1.10 各TQLで要求されるツール資格データ (3/3)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

3. ツール運用要求プロセスとツール運用統合プロセス、および対応する検証/妥当性確認活動の間に作られたツール資格データ

No	名称	TQL				
		1	2	3	4	5
1	ツール運用要求(Tool Operational Requirements)	○	○	○	○	○
2	ツールインストール報告(Tool Installation Report)	○	○	○	○	○
3	ツール運用要求検証/妥当性確認ケース・手順 (Tool Operational Verification and Validation Cases and Procedures)	○	○	○	○	○
4	ツール運用要求検証/妥当性確認結果 (Tool Operational Verification and Validation Results)	○	○	○	○	○

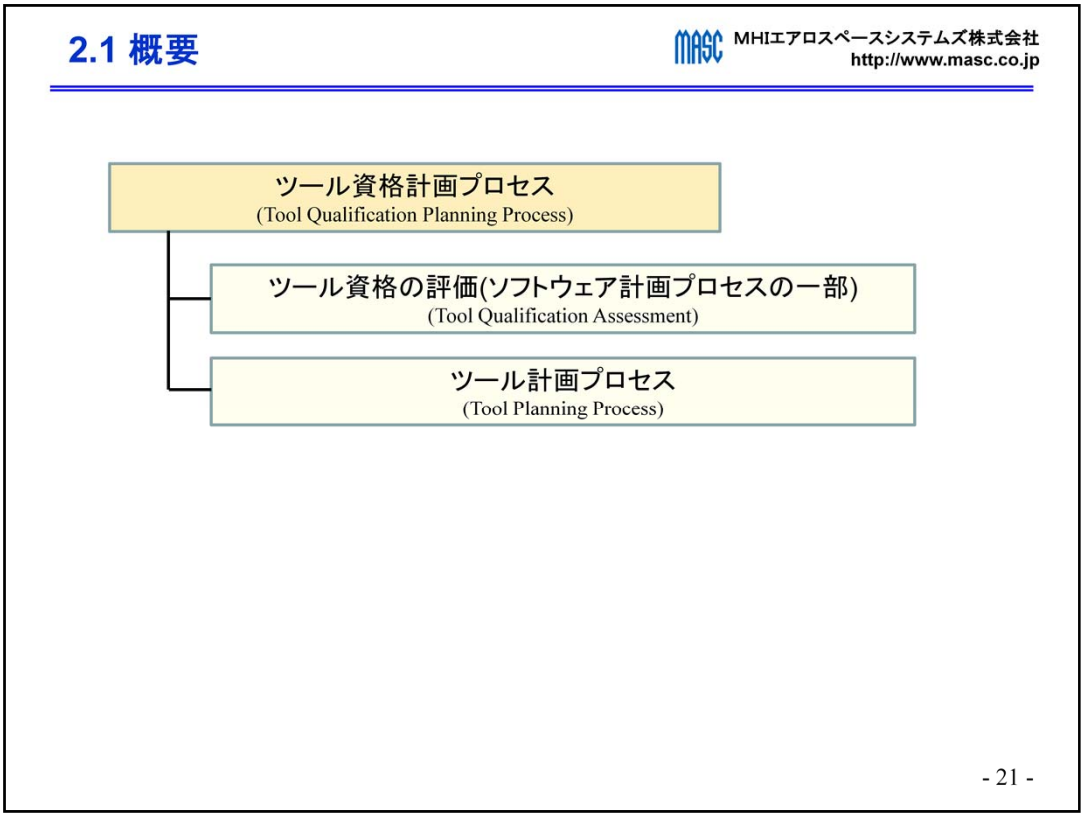
2. ツール資格計画プロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

ツール資格計画プロセス
(Tool Qualification Planning Process)

1. 概要
2. 目的
3. ツール資格データ

【4】



【4.0】

《4.0》ツール資格計画プロセス(Tool Qualification Planning Process)

この章ではツール資格計画プロセスの目的(Objectives)と活動について説明する。ツール資格計画プロセスの間、ツールは識別され、ソフトウェアライフサイクルプロセスでのその影響が評価され、完全なツールライフサイクルのツール開発/検証/インテグラルプロセスが記述される。

ツール資格計画プロセスとしては次があげられる。

(1)ソフトウェア計画プロセスの一部としてのツール資格評価(付録Aの表T-0の一部の"計画プロセス"を参照)

(2)ツール計画プロセス(付録Aの表T-1の全てを参照)。

付録Aの表T-0とT-1に各TQLに対するツール資格計画プロセスの目的と成果物を要約する。

《4.0》

《4.2》ツールライフサイクル定義(Tool Life Cycle Definition)

ツール計画プロセスの間、各プロセスにおける活動の選択、活動のための手順の特定、活動のための責任の割り当てにより、プロジェクトは一つ以上のライフサイクルを定義する。

ツールライフサイクルプロセスは:

a. ツール開発プロセスとインテグラルプロセスの活動を定義しまとめるツール計画プロセス
b. ツールを製造するツール開発プロセス
c. ツールライフサイクルプロセスとその成果物の正当性、管理、信頼を確認するインテグラルプロセス。インテグラルプロセスはツール検証プロセス、ツール形態管理プロセス、ツール品質保証プロセス、資格化連絡調整プロセスからなる。インテグラルプロセスはツールライフサイクルプロセスを通してツール開発プロセスとともに実

施されると理解する事が重要である。

DO-330は推奨されるツールライフサイクルとそれらの相互作用を規定しない。プロセスの分離はそれを実施する組織の構造を暗に意図したものではない。各ツールにおいて、ツールライフサイクルはこれらのプロセスを含む。

ツールライフサイクルの定義は移行条件を含む、それはプロセスを開始するか再開始するかを決定することに利用される。各プロセスは入力に基づいて成果物を作成する活動を実施する。プロセスは他のプロセスへのフィードバックを作成し、他からフィードバックを受けるかもしれない。フィードバックの定義には受け取るプロセスによりどのような情報が認識され、管理され、解決されるかがある。フィードバックの例は不適合報告である。

移行条件はツール開発プロセスとインテグラルプロセスの計画されたシーケンスに依存するだろう、そしてTQLに影響されるかもしれない。プロセスのために確立された移行条件が満たされた場合、プロセスへのすべての入力はそのプロセスが開始可能になる前に完全である必要はない。

部分的な入力に基づいてプロセスが進む場合、それらが移行条件を満足するか確認するためにプロセスへの入力は調査されねばならない。ツール開発及びツール検証プロセスの前の成果物がまだ妥当であることを決定するためにプロセスへの継続する入力は調査されねばならない。

《4.2》

2.2 目的(Objectives) 1/3

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

2.2.1 Table T-0 Tool Operational Process

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
1	ツール資格の必要性が確立されている。	4.1	Note 1	○	○	○	○	○	PSAC内のツール固有情報	10.1.1	①	①	①	①	①

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

- 22 -

【Table T-0】

《4.1》ツール資格必要性の決定

ソフトウェア計画プロセスの間に:

・ソフトウェアライフサイクルプロセスの範囲で利用されるツールが識別される
・各ツールの意図された用途が記述される
・ツール資格の必要性が定義される
・TQLが決定される。
・ツール資格のステークホルダーと彼らに与えられた役割と責任が識別される
・ツール運用環境が記述される

もし複数のツール運用環境がある場合、全てのそのような環境は記述される。これら全ての項目はPSACの追加考慮事項の章で説明せねばならない。PSACはソフトウェアライフサイクルプロセスにおけるツールの用途とツール資格の必要性を説明している。PSACに示されるべきツールの特徴はこの資料の10.1.1章を参照。

《4.1》

2.2 目的(Objectives) 2/3

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

2.2.2 Table T-1 Tool Planning Process(1/2)

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
1	ツール開発プロセス、インテグラルプロセスが定義されている。	4.3.a	4.4.a	○	○	○	○								
2	ツールプロセス間の移行基準、相互関係、シーケンス処理が定義されている。	4.3.b	4.4.a	○	○	○			ツール資格計画	10.1.2	①	①	①	①	
									ツール開発計画	10.1.3	①	①	②	②	
3	ツール開発環境が選択され、定義されている。	4.3.c	4.4.c	○	○	○			ツール検証計画	10.1.4	①	①	②	②	
									ツール形態管理計画	10.1.5	①	①	②	②	
4	追加の考慮事項が示されている。	4.3.d	4.4.a 4.4.e	○	○	○	○		ツール品質保証計画	10.1.6	①	①	②	②	

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

- 23 -

【Table T-1】

《4.3》ツール計画プロセスの目的(Tool Planning Process Objectives)

ツール計画プロセスの目的は下記である。

a. PASCに規定されるようにその意図された用途に準拠するツールライフサイクルプロセスを定義する、それは前の4.1章に示された項目を含む。
b. プロセスとそのシーケンス処理、フィードバックメカニズム、そして移行条件の相互関係を含むツールのライフサイクルを決定する。
c. 各ツールライフサイクルプロセスの活動に利用される手法とツールを含むツール開発環境を識別する。
d. 必要であれば、DO-330の11章で説明されている事項やツールライフサイクルプロセスのフレームワークで利用されるすべてのツールの資格化の必要性のような追加考慮事項を示す。
e. ツール開発標準を定義する。
f. ツール計画がDO-330の10章に適合することを確かにする。
g. ツール計画の開発と改訂を調整する。

《4.3》

《4.4》ツール計画プロセスの活動(Tool Planning Process Activities)

DO-330の目的(Objectives)を満たすために、効率的な計画作業が必要とされる。このプロセスのための活動には下記があげられる。

a. 完全なツールライフサイクルをカバーするTQP、ツール開発計画、ツール検証計画、ツール品質保証計画、ツール形態管理計画は開発されるべきである。これらの計画は特有のプロジェクト要求に適切なように分離又は

統合していてもよい。例として、ツールサプライヤは資格化可能ツールを提案したり、ツール開発プロセスのみの計画を作ってもよい(COTSツール資格のための11.3章を参照) 、しかしツール運用要求定義とツール運用統合プロセスの記述はツール計画群とは分かれて述べられるだろう。各計画と関連する標準は下記に簡潔に記載され、10章で詳細に記述される。

1. TQP(10.1.2参照)は提案されたツールライフサイクルと開発手法を合意のため認証機関に伝達するための主な手段となる。TQPはDO-330とその他の適切なガイダンス(例えば、ドメイン又はプロジェクト特有の資料)への適合手段を規定する。

2. ツール開発計画(10.1.3参照)はツールライフサイクル、ツール開発環境とプロセス、およびツール開発プロセス目的(Objectives)を満たす手法を定義する。

3. ツール検証計画(10.1.4参照)はツール検証プロセスの目的(Objectives)を満たす手法を定義する。

4. ツール形態管理計画(10.1.5参照)はツール形態管理プロセス目的(Objectives)を満たす手法を定義する。

5. ツール品質保証計画(10.1.6参照)はツール品質保証プロセス目的(Objectives)を満たす手法を定義する。

b. ツール開発標準は開発されなければならない。これらの標準の目的はすべての開発プロセスのための規則や制約を規定することである。ツール開発標準はツール要求標準(10.1.7参照)、ツール設計標準(10.1.8参照)、ツールコード標準(10.1.9参照)を含む。ツール検証プロセスはこれらの標準を意図された成果物とプロセスの実成果物の適合性を評価するための基礎として利用する。

c. ツール検証環境は定義されるべきである。検証環境はツール運用環境の代表例となるよう示されなければならない。オペレーティングシステムや、追加のハードウェア、追加のソフトウェアコンポーネントなどを識別することを気に掛けるべきである。もし潜在的に複数のツール運用環境(例えば、特定の運用要求に依存して、ツールは異なるバージョンのOSの複数のプラットフォームで使用されるかもしれない。)がある場合、いくつかのツール検証環境をもつことは必要かもしれないと注意されるべきである。

d. 計画と標準がDO-330のガイダンスに準拠し、それらを実行する手段が存在することを確認するために、ツール計画プロセスのレビューは実施されなければならない。

e. ツールライフサイクルプロセスのフレームワーク内で使用されるすべてのツールの評価は、これらのツールの資格化の必要性を識別するために、実施されなければならない。6章で明確にされているように検証された成果物がなくツールの利用によりDO-330のプロセスを削除、減少、自動化するとき、これらのツール認定が必要である。ツールの生成物にエラーをもたらす可能性のあるツールでは、適切なTQLは開発されているツールと同じである。ツールの生成物にエラーをもたらす可能性がなく、ツールライフサイクルデータ内でエラーを検知することに失敗するかもしれないツールでは、適切なTQLはTQL-5である。

《4.4》

2.2 目的(Objectives) 3/3

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

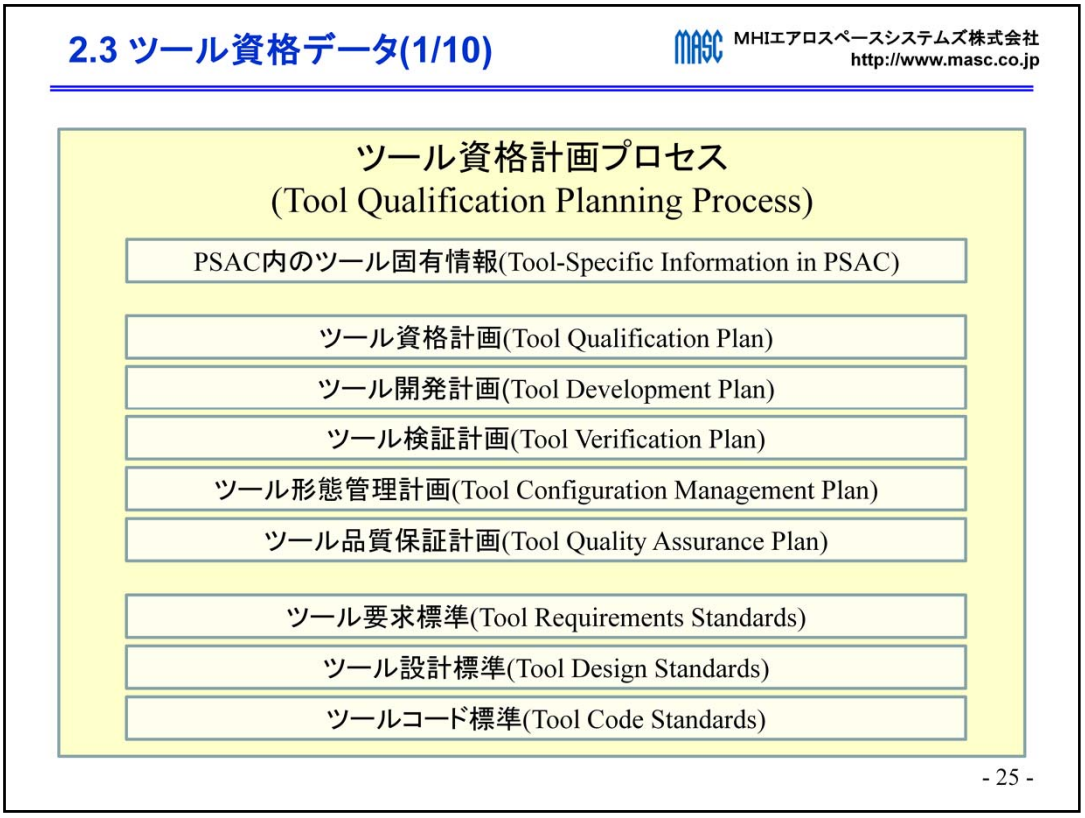
2.2.2 Table T-1 Tool Planning Process(2/2)

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
5	ツール開発標準が定義されている。	4.3.e	4.4.b	○	○	○			ツール要求標準 ツール設計標準 ツールコード標準	10.1.7 10.1.8 10.1.9	① ① ①	① ① ①	② ② ②		
6	ツール計画がDO-330に準拠している。	4.3.f	4.4.d	○	○	○			ツール検証結果	10.2.6	②	②	②		
7	ツール計画の開発と改訂が調整されている。	4.3.g	4.4.d	○	○	○			ツール検証結果	10.2.6	②	②	②		

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

- 24 -

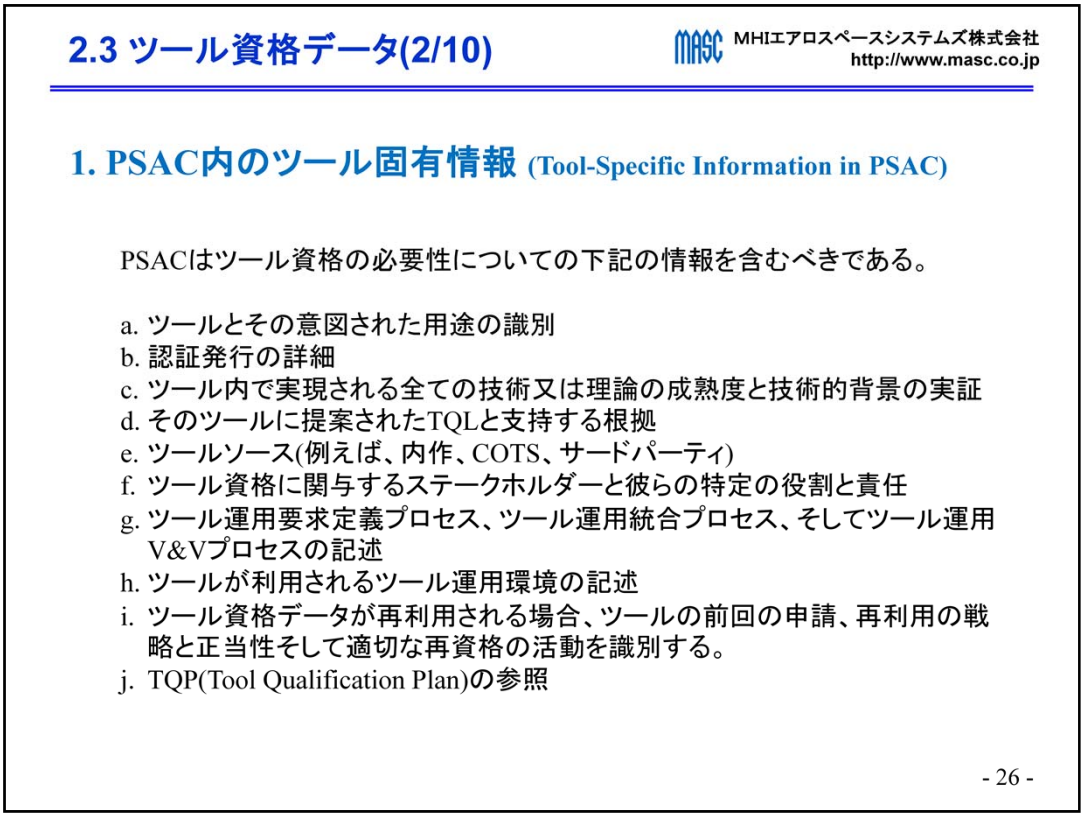
【Table T-1】



【10】

以降、ツール資格計画プロセスの成果物について説明する。

前述したように、成果物（文書）としては、PSAC内に記述する項目、計画に係わる5種類の文書、標準に関わる3種類の文書がある。



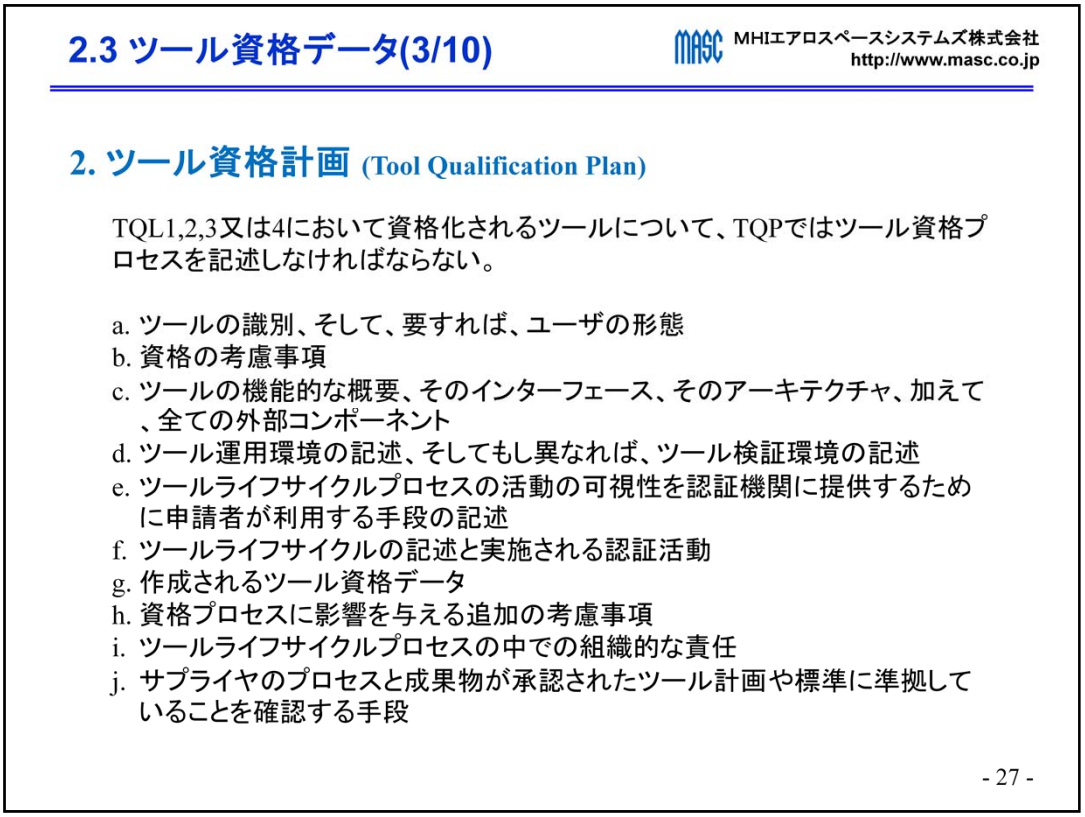
【10.1.1】

《10.1.1》 PSAC内のツール固有情報(Tool-Specific Information in PSAC)

PSACはツール資格の必要性についての下記の情報を含むべきである。

a. ツールとその意図された用途の識別、ソフトウェアライフサイクルプロセスでのその影響を含む
b. プロセスの削除、削減、自動化のためのツール利用を通して求められる認証発行の詳細
c. その適用性を示すためにツール内で実現される全ての技術又は理論(例えば、数学的な理論)の成熟度と技術的背景の実証
d. そのツールに提案されたTQLと支持する根拠
e. ツールソース(例えば、内作、COTS、サードパーティ)
f. ツール資格に関与するステークホルダーと彼らの特定の役割と責任、誰に特定の目的を満足させる責任があるのかを含む。
g. ツール運用要求定義プロセス(5.1参照)、ツール運用統合プロセス(5.3参照)、そしてツール運用V&Vプロセス(6.2参照)の記述(又はこれらのプロセスが記載されるであろう場所への参照)。
h. ツールが利用されるツール運用環境の記述
i. ツール資格データが再利用される場合、ツールの前回の申請、再利用の戦略と正当性そして適切な再資格の活動を識別する。サードパーティツール又はCOTSツールの場合、前回の申請についての情報は、ツールのユーザから入手不可能であるので、サプライヤから提供を受けることができる。既に資格化されたツールそしてCOTSツールの再利用については11.2そして11.3章を参照。
j. TQPの参照、又は、TQPが作成されていなければ (TQL-5について)、ツール資格を支援するデータへの参照

《10.1.1》



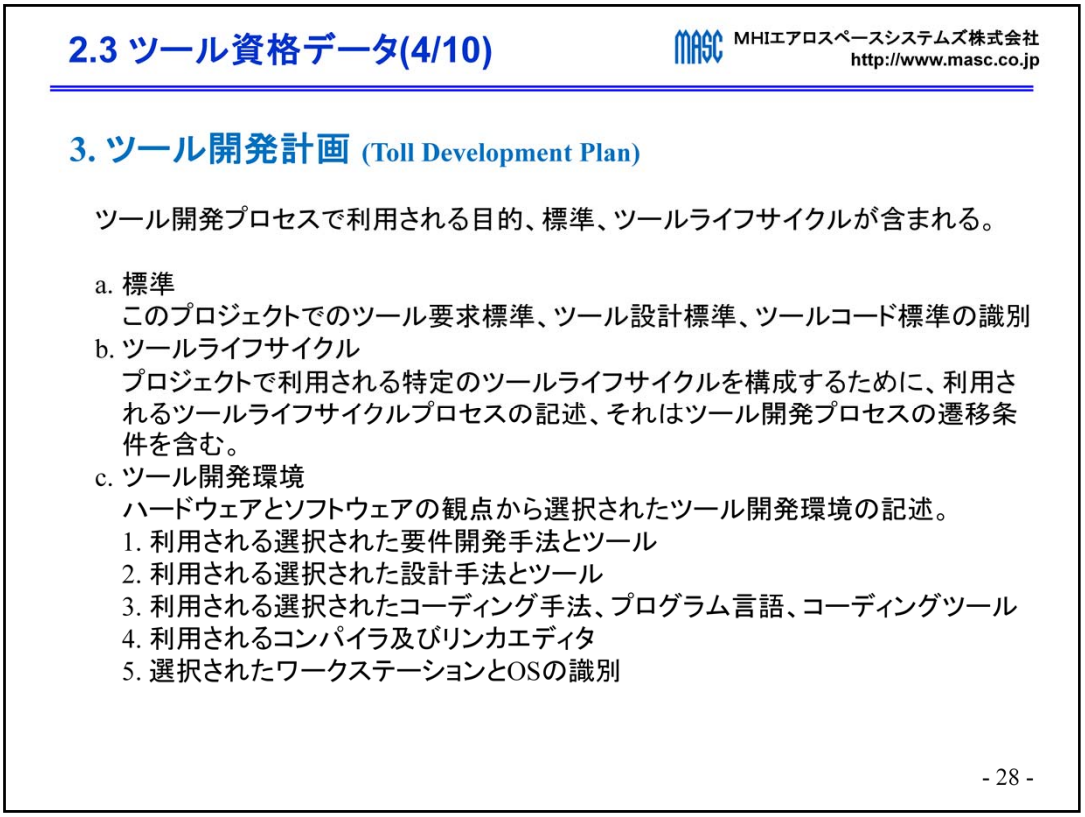
【10.1.2】

《10.1.2》ツール資格計画(Tool Qualification Plan)

TQL1,2,3又は4において資格化されるツールについて、TQPではツール資格プロセスを記述しなければならない。この計画は以下を含む。

a. ツールの識別、そして、要すれば、ユーザの形態
b. 資格の考慮事項、提案されたTQL、DO-330の目的を準拠させる手法を含む
c. ツールの機能的な概要、そのインターフェース、そのアーキテクチャ、加えて、全ての外部コンポーネントが識別されるべきである
d. ツール運用環境の記述、そしてもし異なれば、ツール検証環境の記述
e. ツールレビューを計画するため、ツールライフサイクルプロセスの活動の可視性を認証機関に提供するために申請者が利用する手段の記述
f. ツールライフサイクルの記述と実施される認証活動
g. 作成されるツール資格データ
h. 資格プロセスに影響を与える追加の考慮事項、例えば、使用されないコード、COTSツール、再利用、(ツールの開発又は検証に利用される他のツールの)ツール資格、資格化の代替手段、ツール使用履歴、DO-330の2.0章の最終段落でのツール決定の確認手段
i. ツールライフサイクルプロセスの中での組織的な責任
j. サプライヤを用いる場合、サプライヤのプロセスと成果物が承認されたツール計画や標準に準拠していることを確認する手段

《10.1.2》



【10.1.3】

《10.1.3》ツール開発計画(Tool Development Plan)

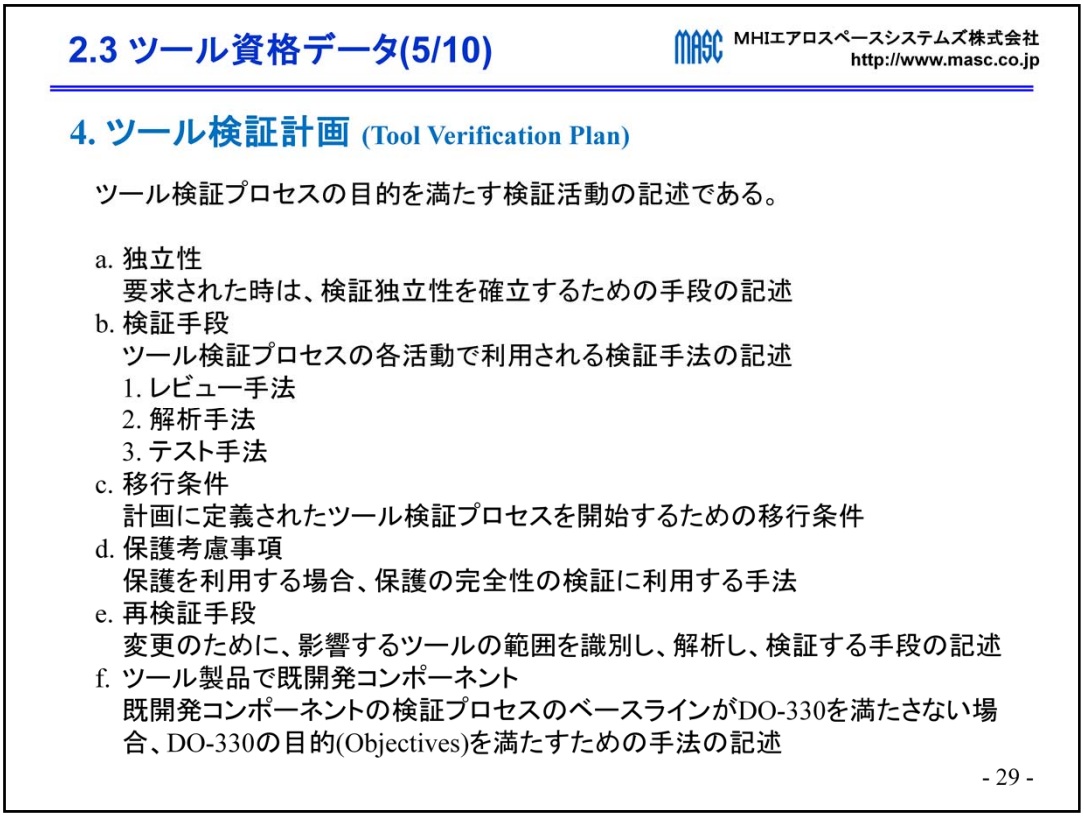
ツール開発計画にはツール開発プロセスで利用される目的、標準、ツールライフサイクルが含まれる。
この計画は下記を含むべきである。

a. 標準
このプロジェクトでのツール要求標準、ツール設計標準、ツールコード標準の識別

b. ツールライフサイクル
プロジェクトで利用される特定のツールライフサイクルを構成するために、利用されるツールライフサイクルプロセスの記述、それはツール開発プロセスの遷移条件を含む。この記述はTQPで提供される概要とは異なり、ツールライフサイクルプロセスの適切な履行を確認するために十分に詳細な必要性のある開発活動の記述を提供する。

c. ツール開発環境
ハードウェアとソフトウェアの観点から選択されたツール開発環境の記述、これは下記を含む。
1. 利用される選択された要件開発手法とツール
2. 利用される選択された設計手法とツール
3. 利用される選択されたコーディング手法、プログラム言語、コーディングツール
4. 利用されるコンパイラ及びリンカエディタ
5. 選択されたワークステーションとOSの識別

《10.1.3》



【10.1.4】

《10.1.4》ツール検証計画(Tool Verification Plan)

ツール検証計画はツール検証プロセスの目的を満たす検証活動の記述である。これらの手順は付録 A表に定義されるようにTQLにより様々である。

この計画は下記を含まねばならない。

a. 独立性
要求された時は、検証独立性を確立するための手段の記述

b. 検証手段
ツール検証プロセスの各活動で利用される検証手法の記述、これは下記を含む。
1. レビュー手法、チェックリストや他の支援を含む
2. 解析手法、トレーサビリティやカバレッジ解析を含む
3. テスト手法、テストケースの選択、利用されるテスト手順、作成されるテストデータのための手法を含む

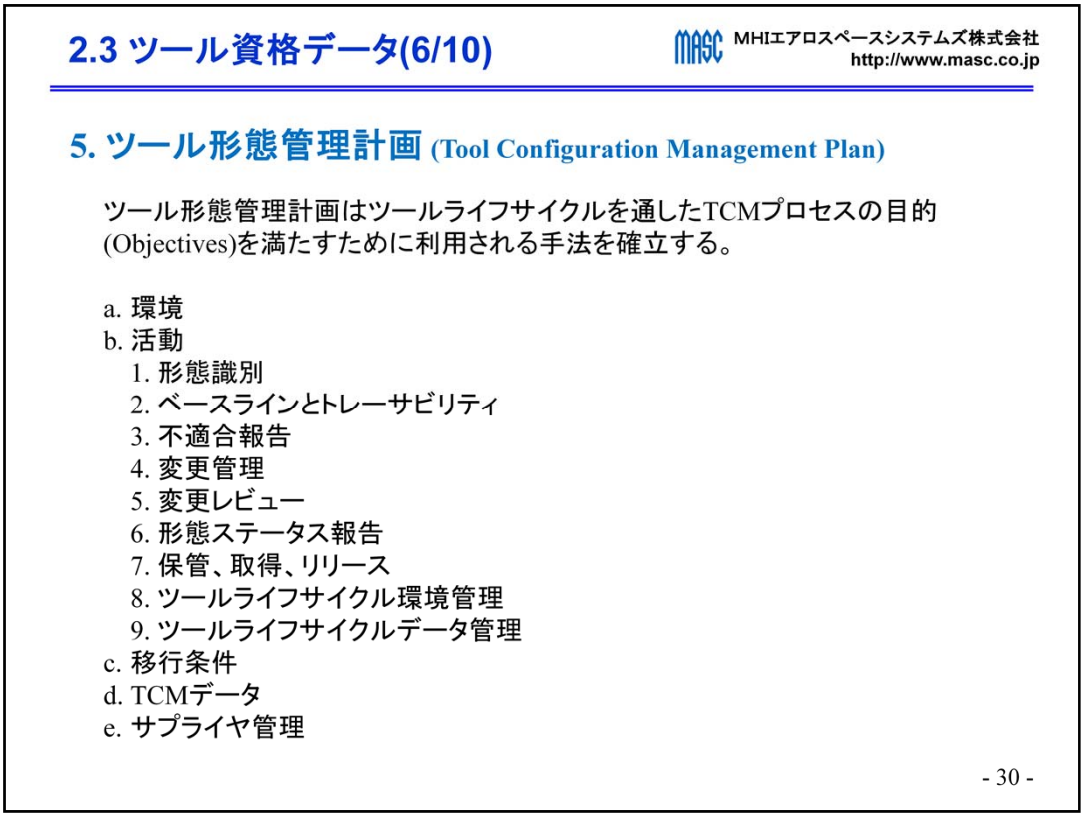
c. 移行条件
計画に定義されたツール検証プロセスを開始するための移行条件

d. 保護考慮事項
保護を利用する場合、保護の完全性の検証に利用する手法

e. 再検証手段
変更のために、影響するツールの範囲を識別し、解析し、検証する手段の記述

f. ツール製品で既開発コンポーネント
これらのコンポーネントのため、検証プロセスの初期の準拠ベースラインがDO-330を満たさない場合、DO-330の目的(Objectives)を満たすための手法の記述

《10.1.4》



【10.1.5】

《10.1.5》ツール形態管理計画(Tool Configuration Management Plan)

ツール形態管理計画はツールライフサイクルを通したTCMプロセスの目的(Objectives)を満たすために利用される手法を確立する。
この計画は下記を含まなければならない。

a. 環境
使用されるTCM環境の記述、これは手順、ツール、手法、標準、組織的責任、そしてインターフェースを含む。

b. 活動
ツールライフサイクルにおけるTCMプロセス活動の記述、これは下記を含む。
1. 形態識別
識別された項目(それらが識別される時)、ツールライフサイクルデータの識別手法
2. ベースラインとトレーサビリティ
ベースラインを確立する手法、どのベースラインが確立され、これらのベースラインがいつ確立されるか、ソフトウェアライブラリの管理、および形態項目とベースラインのトレーサビリティ
3. 不適合報告
ツールとツールライフサイクルプロセスに対するツール不適合報告の内容と識別、それらが記載された時、ツール不適合報告をクローズする手法、変更管理活動との関係
4. 変更管理
管理される形態項目とベースライン、それらが管理されるとき、それらを管理する不適合/変更管理活動、資格化前管理、資格化後管理、ベースラインと形態項目の完全性を保持する手法
5. 変更レビュー
ツールライフサイクルプロセスから又はそれへのフィードバックを取り扱う手法;不適合評価と優先度付、変更の承認、それらの解決の取扱い、変更の適用の手法:不適合報告及び変更管理活動とこれらの手段の関係
6. 形態ステータス報告
形態管理ステータスを報告可能にするために記録されるデータ、そのデータが記録される場所、報告のために取り出すための方法、利用可能になる時期の定義
7. 保管、取得、リリース

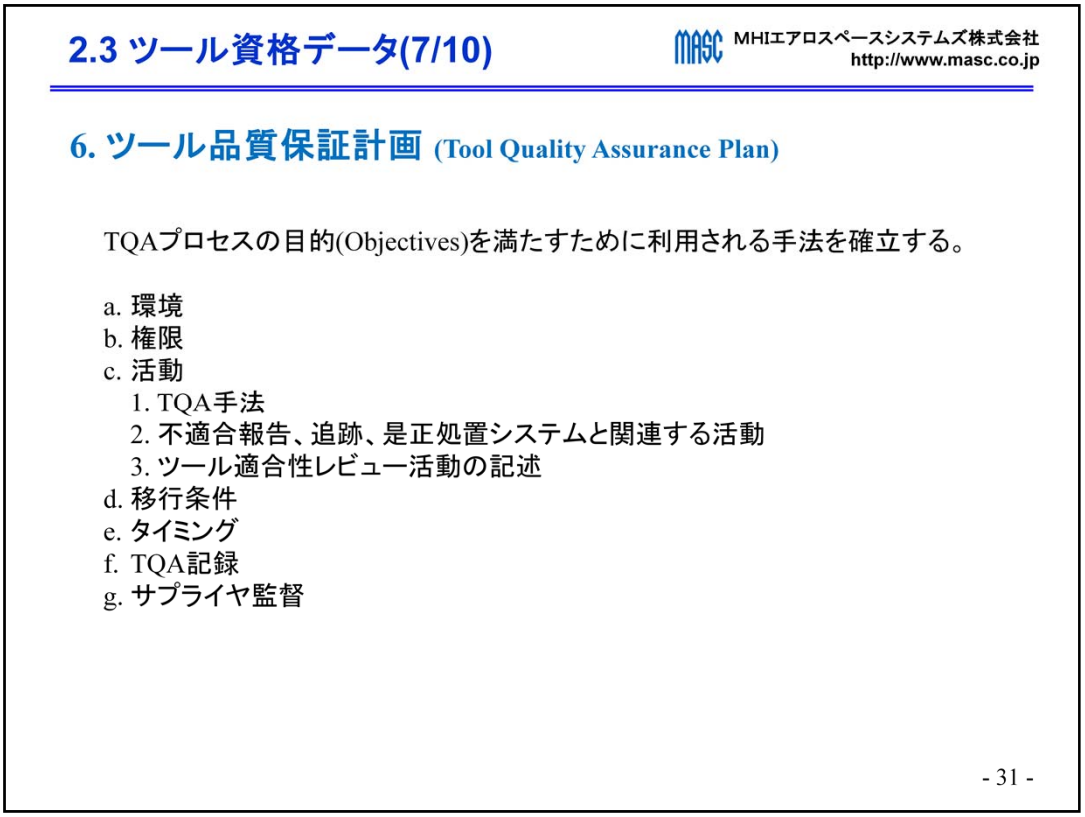
完全性管理、リリース手法、権限、データ保管期限
8. ツールライフサイクル環境管理
上記1から7に示されたツールの開発、ビルド、検証、ロードに利用されるツールのための管理
9. ツールライフサイクルデータ管理
CC1、CC2データに関連する管理

c. 移行条件
TCMプロセスを開始するための移行条件

d. TCMデータ
TCMプロセスで作成されるツールライフサイクルデータの定義、これはTCM記録、ツール形態索引、ツールライフサイクル形態索引を含む。

e. サプライヤ管理
サプライヤにTCMプロセス要件を適用する手段

《10.1.5》



【10.1.6】

《10.1.6》 ツール品質保証計画(Tool Quality Assurance Plan)

TQA計画は、TQAプロセスの目的(Objectives)を満たすために利用される手法を確立する。TQA計画はプロセス改善、メトリクス、前進的な管理手法の説明を含んでもよい。

この計画は下記を含むべきである。

a. 環境
TQA環境の記述、これは範囲、組織的責任、インターフェース、標準、手順、ツール、手法を含む

b. 権限
TQA権限、責任、独立性の記述

c. 活動
各ツールライフサイクルプロセス、およびツールライフサイクルを通して実施されるTQA活動
1. TQA手法、例えば、レビュー、監査、報告、検査、そしてツールライフサイクルプロセスの監視
2. 不適合報告、追跡、是正処置システムと関連する活動
3. ツール適合性レビュー活動の記述

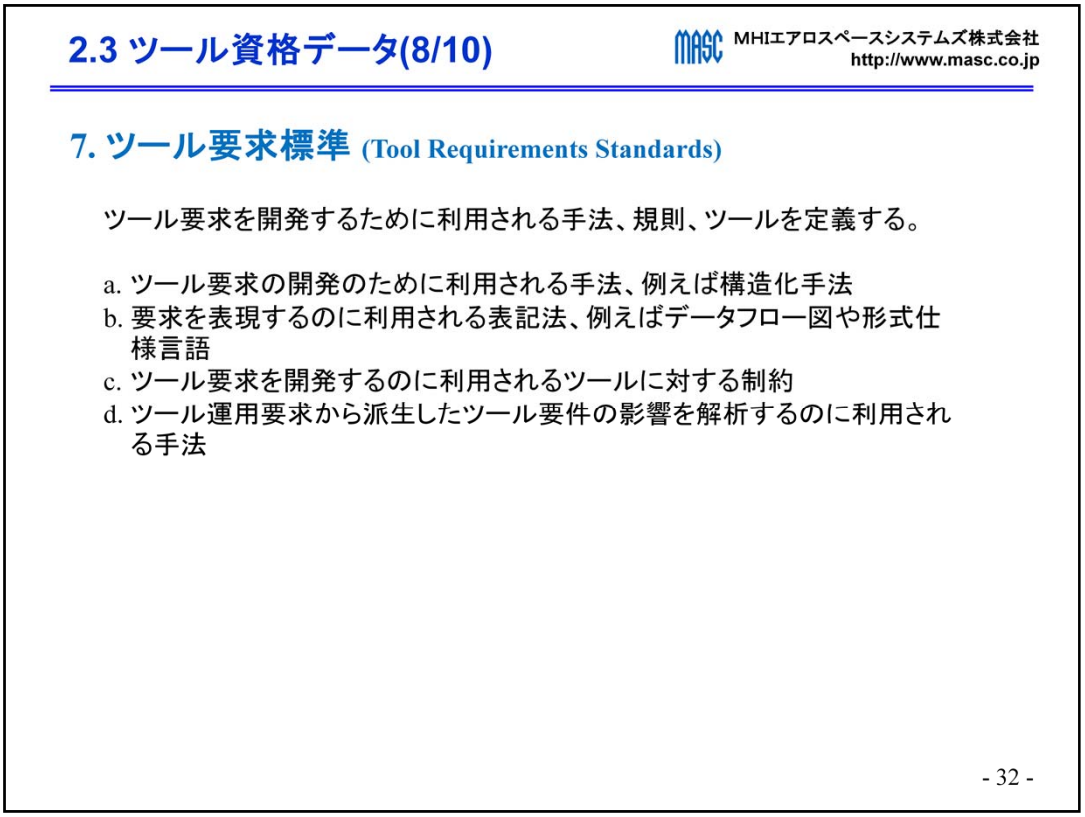
d. 移行条件
TQAプロセスを開始するための移行条件

e. タイミング
ツールライフサイクルプロセスの活動との関係におけるTQAプロセス活動のタイミング

f. TQA記録
TQAプロセスにより作成される記録の定義

g. サプライヤ監督
サプライヤのプロセスと成果物が承認された計画と標準に準拠していることを確認する手法の定義

《10.1.6》



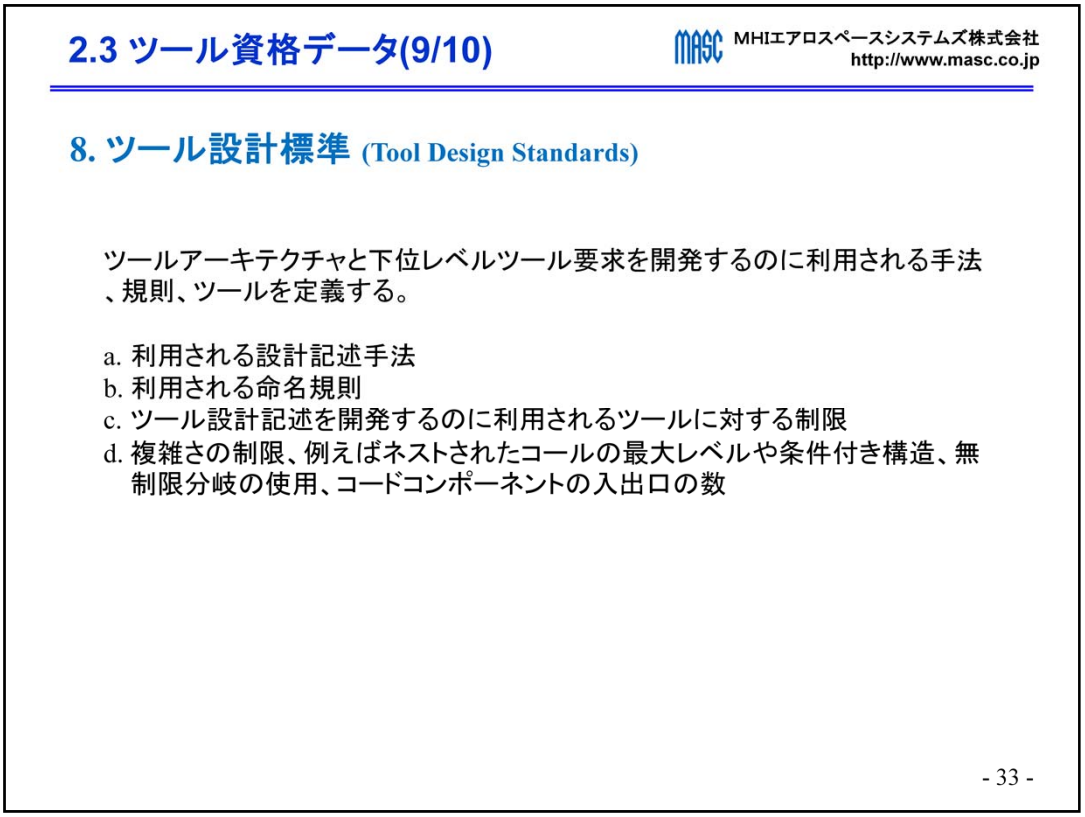
【10.1.7】

《10.1.7》ツール要求標準(Tool Requirements Standards)

ツール要求標準の目的はツール要求を開発するために利用される手法、規則、ツールの定義である。
この標準は下記を含まなければならない。

a. ツール要求の開発のために利用される手法、例えば構造化手法
b. 要求を表現するのに利用される表記法、例えばデータフロー図や形式仕様言語
c. ツール要求を開発するのに利用されるツールに対する制約
d. ツール運用要求(5.2.1.2.h参照)から派生したツール要件の影響を解析するのに利用される手法

《10.1.7》



【10.1.8】

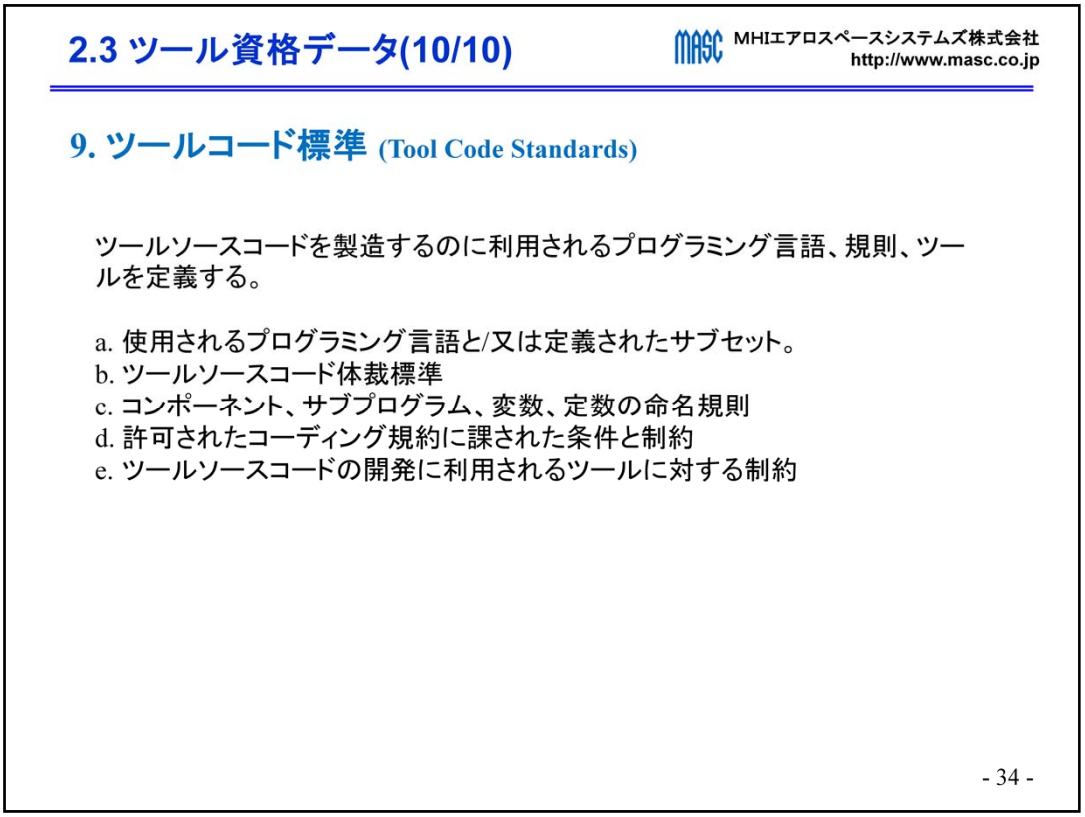
《10.1.8》ツール設計標準(Tool Design Standards)

ツール設計標準の目的はツールアーキテクチャと下位レベルツール要求を開発するのに利用される手法、規則、ツールを定義することである。
これらの標準は下記を含まなければならない。

a. 利用される設計記述手法
b. 利用される命名規則
c. ツール設計記述を開発するのに利用されるツールに対する制限
d. 複雑さの制限、例えばネストされたコールの最大レベルや条件付き構造、無制限分岐の使用、コードコンポーネントの入出口の数

注意:いくつかの場合、ツール要求標準はツール設計標準よりも下位レベルツール要求のために利用されるだろう。

《10.1.8》



【10.1.9】

《10.1.9》 ツールコード標準(Tool Code Standards)

ツールコード標準の目的はツールソースコードを製造するのに利用されるプログラミング言語、規則、ツールを定義することである。

これらの標準は下記を含まねばならない。

a. 使用されるプログラミング言語と/又は定義されたサブセット。プログラミング言語に対し、言語の構文、制御の振る舞い、データの振る舞い、副作用を明白に定義するデータへの参照、これは言語のいくつかの機能の利用の制限を求めるかもしれない。
b. ツールソースコード体裁標準(例えば、行長制限、インデント、空白行利用)とツールソースコード情報管理標準(例えば、作者の名前、改訂履歴、入力と出力、影響するグローバルデータ)
c. コンポーネント、サブプログラム、変数、定数の命名規則
d. 許可されたコーディング規約に課された条件と制約、例えば、ソフトウェアコンポーネント間の結合度、論理的又は数値的式の複雑度、それらの利用の論理的根拠
e. ツールソースコードの開発に利用されるツールに対する制約

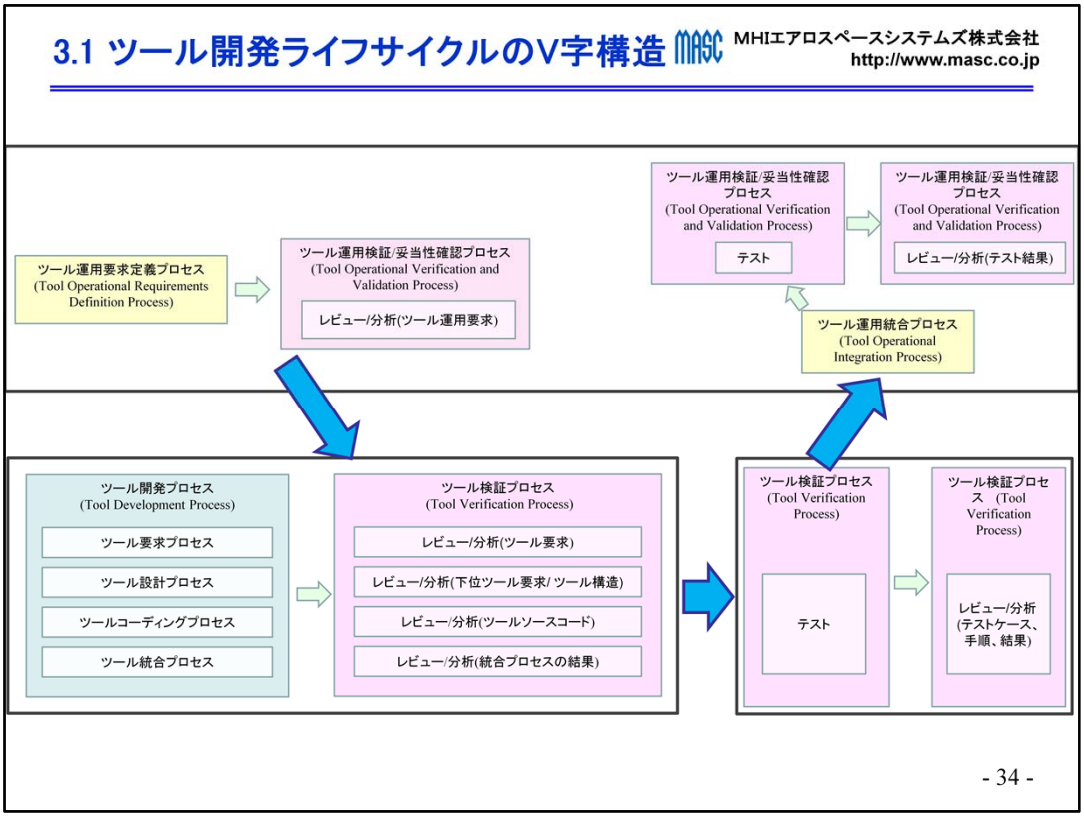
《10.1.9》

3.0 ツール開発ライフサイクル

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

ツール開発ライフサイクル
(Tool Development Life Cycle)

1. ツール開発ライフサイクルのV字構造
2. ツール運用要求定義プロセス
3. ツール統合プロセス



【5.0】

この図は、ツール開発ライフサイクルのプロセス全体像を、一般的に言われるV字のプロセスとして表している。

上流左側のツール運用要求定義プロセスは、ツールがどのように運用されるのかを明らかし、それらをツール運用要求としてまとめる。

ツール運用要求はツール運用検証/妥当性プロセスにおいてレビュー/分析される。

続くV字左側のツール開発プロセスは、順を追ってのツール開発が行われる。

ここで作成される成果物は、開発プロセスと並行して行われるツール検証プロセスにおいてレビュー/分析される。

V時右側のプロセスにおいて、ツール開発プロセスで作成されたツール実行可能オブジェクトコードをインプットとして、テストが行われる。

これは、ツール開発プロセスで作成された要求(ツール要求、下位ツール要求、ツール構造)に従うことを保証するためテストである。

また、ここで作成された成果物はレビュー/分析の対象となる。

上流右側のツール運用統合プロセスは、ツールを運用環境にインストールするものである。

実際の運用環境にインストールされたツールを対象とし、ツール運用検証/妥当性確認プロセスにおいて、

ツール運用要求を満たすことを保証するためテストが行われる。

また、テスト結果はレビュー/分析される。

《5.0》ツール開発ライフライフサイクルとプロセス(TOOL DEVELOPMENT LIFE CYCLE AND PROCESS)

このセクションではツール開発ライフサイクルの目的と活動について論じる。ツール開発プロセスは計画プロセス(4を参照)及びツール開発計画(10.1.3を参照)によって定義される通りに適用される。特有のツール向けのツー

ル開発ライフサイクルは、TQLに基づき作成されてもよい。ツール資格プロセスの主要目的は、ツールがその要求を満たし、ソフトウェアライフサイクルプロセスの要求に準拠していることを確認することである。それ故、ソフトウェアライフサイクルプロセスの観点からの要求はツール運用要求で定義され、ツールを開発するために必要な機能性と特性はツール要求で定義される。ツール開発ライフサイクルには、図5-1及び以下で述べられるように、3つの大きなプロセスがある。これらのプロセスはリニアウォーターフォールライフサクルモデルの中で記述されているが、他のライフサイクルモデルが使われても良いことに注意しなければならない。

ここでは各プロセスについて簡潔に記述し、詳細は後のセクション5.1から5.3で述べる。

a. ツール運用要求定義プロセス(5.1を参照): ツール運用要求は、ソフトウェアライフサイクルプロセス内でどのようにツールが使われるかを明らかにしなければならない。それはツールを開発するために必要な全ての要求を提供しなくても良い。ツール運用要求の詳述の量はツールとその用途に依存する。ツール運用要求の妥当性確認及び検証は、ツールがソフトウェアライフサイクルの要求を満たすことを確認するために必要である。ツール運用要求定義プロセスはツール開発計画に記述される。このプロセスの成果物はツール運用要求である。

b. ツール開発プロセス(5.2を参照): ツール開発プロセスはTQPとツール開発計画によって定義される通りに適用される。ツール開発プロセスには以下の項目がある。

・ツール要求プロセス

・ツール設計プロセス

・ツールコーディングプロセス

・ツール統合プロセス

ツール要求プロセスはツール要求を作り出す。ツール要求はツールを開発するために利用される要求である。ツール要求はツール運用要求の分析から作成されなければならない。しかしながら、多種多様なアプリケーションのため開発されツールもあり、それらは特有の運用要求に基づかないかもしれない。これらのツールに関するより多くの情報についてはセクション11.3を参照せよ。

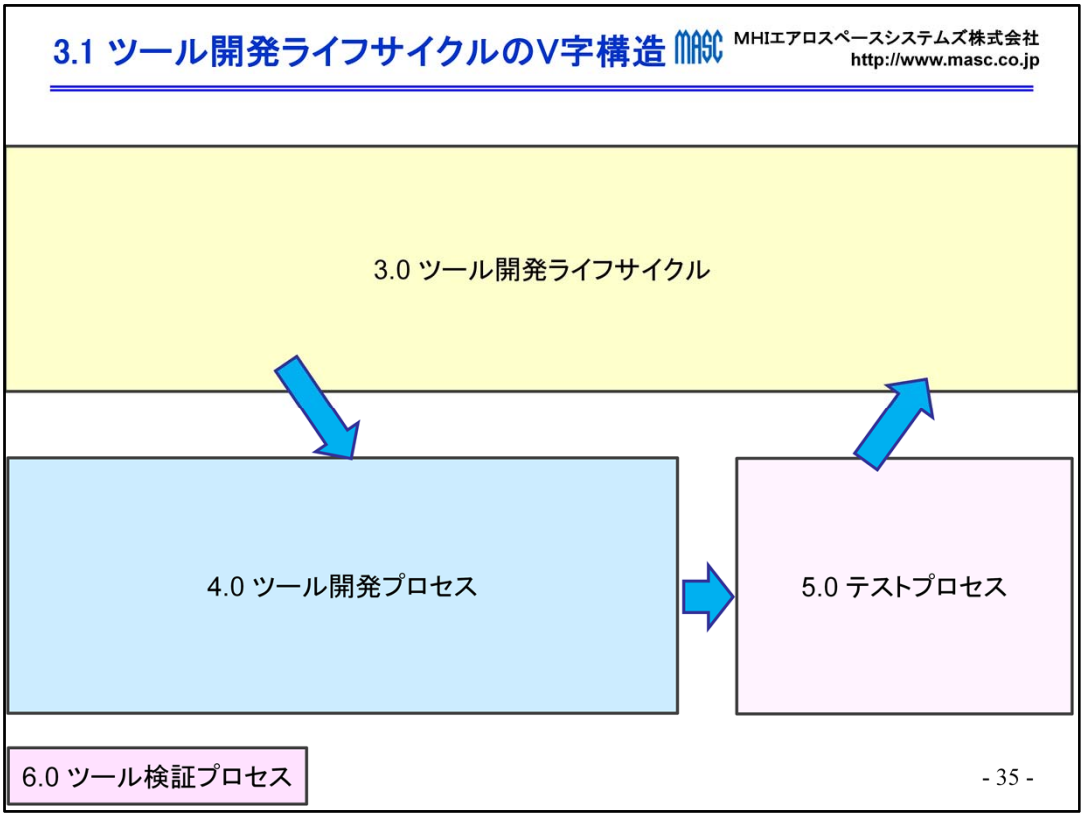
ツール設計記述にはツール構造が含まれ、下位ツール要求の1つ以上のレベルを生成しても良い。しかしながら、もしツールソースコードがツール要求から直接生成され、ツール要求もまた下位要求とみなされるなら、下位要求のガイダンスもまたはツール要求を適用する。ソースコードはツール構造と下位ツール要求から実現される。

ツール実行可能オブジェクトコードはツール開発環境内で生成される。

Annex Aの表T-2 はTQLに基づくツール開発プロセスの目的と成果物の要約である。

c. ツール運用統合プロセス (5.3を参照): ツール運用統合プロセスはツール計画によって定義される通りに適用される。ツール運用統合プロセスへの入力はツール実行可能オブジェクトコード、取り扱い説明書(user instructions)、インストール説明書である。それらはツール利用法及びツール運用環境へのインストールに関するツール開発プロセスを通して作成される。ツール運用統合プロセスの成果物は、ツール運用環境にインストールされるツール実行可能オブジェクトコードである。

《5.0》



本資料の章構成を示す。

セクション3では、ツール開発ライフサイクルとして、
ツール運用要求定義プロセス、ツール統合プロセス、それに関連するツール運用検証/妥当性確認プロセスについて述べる。

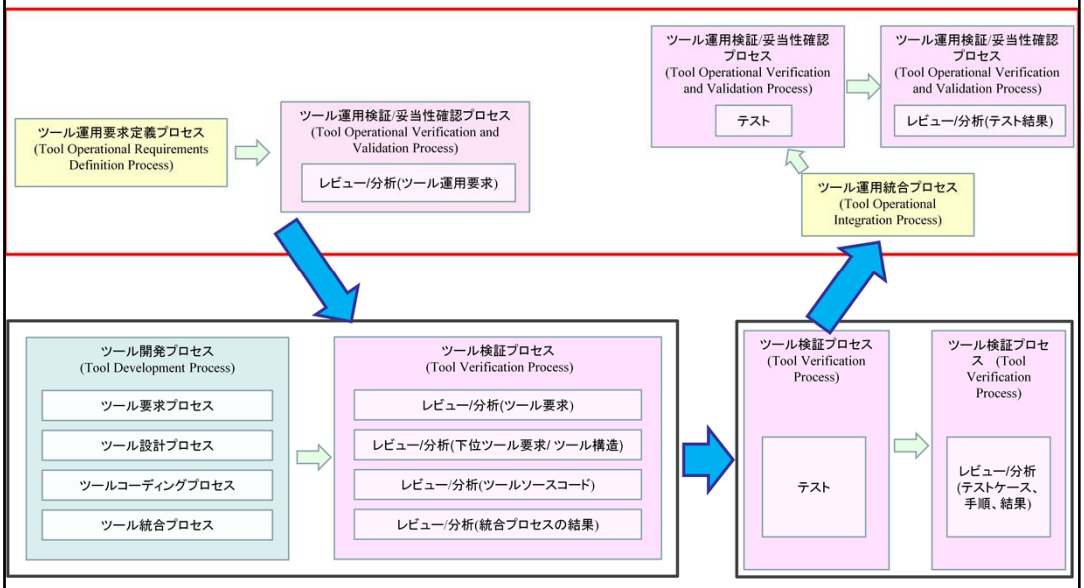
セクション4では、ツール開発プロセスと、関連するツール検証プロセスについて述べます。

セクション5では、テストプロセスについて述べる。

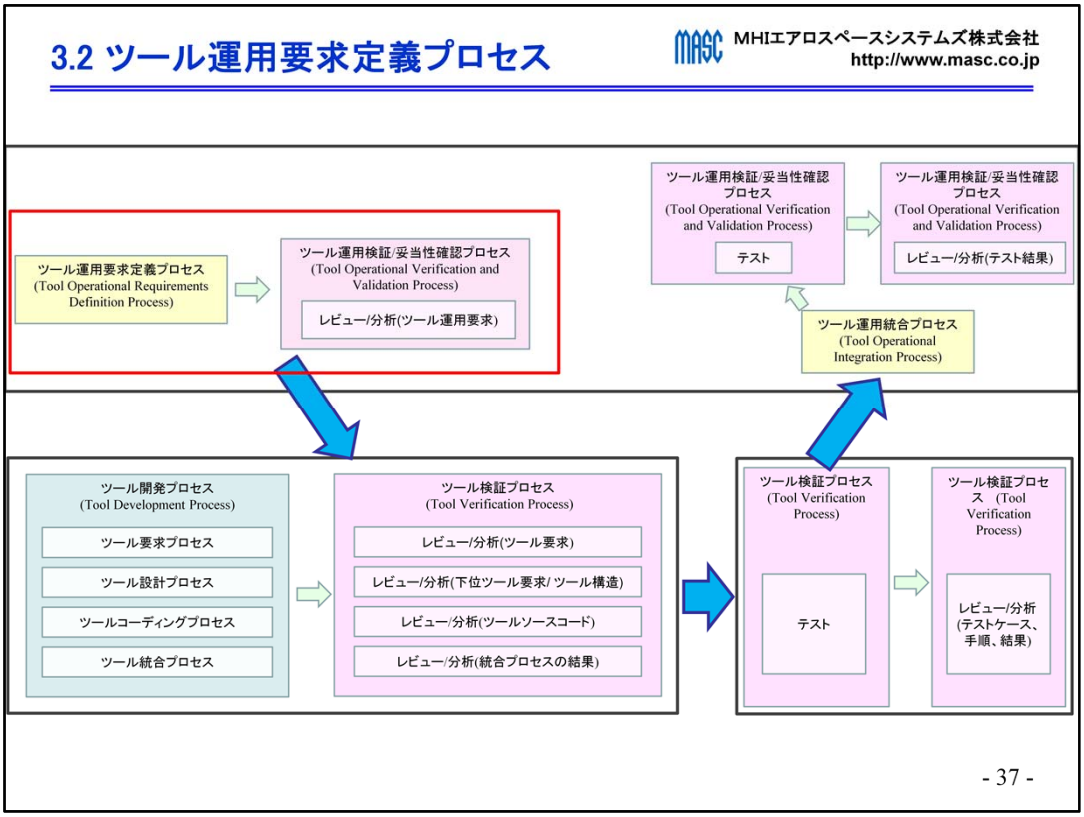
セクション6では、3~5のプロセスで述べられなかったツール検証プロセスの活動に関して述べる。

3.2 ツール開発ライフサイクル

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp



- 36 -



【5.1】

まず、ツール要求定義プロセス(Tool Operational Requirements Definition Process)について説明する。

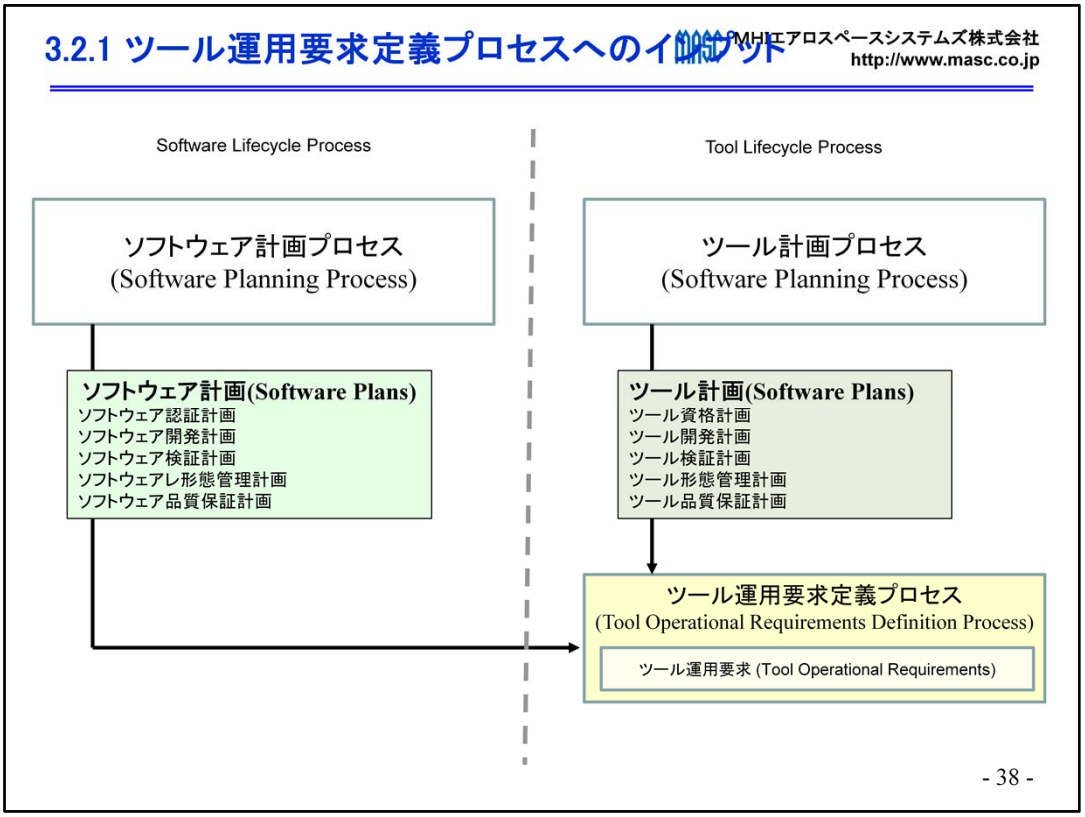
ツール要求定義プロセスは、ソフトウェア計画とツール計画をインプットとして、
どのようにツールが利用されるのかを明らかにする。
これらのアウトプットは成果物として、ツール運用要求(Tool Operational Requirements)にまとめられる。

ソフトウェア計画プロセス(Software Planning Process)プロセスより以下をインプットとして受け取る。
(a)　ソフトウェア計画(software plans)
ツール資格計画プロセス(Tool Qualification Planning Process)より以下をインプットとして受け取る。
(a)　ツール計画(tool plans)

《5.1》ツール運用要求定義プロセス

ツール運用要求は、ソフトウェアライフサイクルプロセスにおいて、どのようにツールが利用されるのかを明らかにする。ソフトウェア計画とツール計画はこのプロセスへの入力である。ツール運用要求はこのプロセスの主要な成果物である(10.3.1を参照)。Annex AのTable T-0の”ツール運用要求プロセス”の部分は、TQLに基づきプロセスの目的と成果物を要約している。

《5.1》

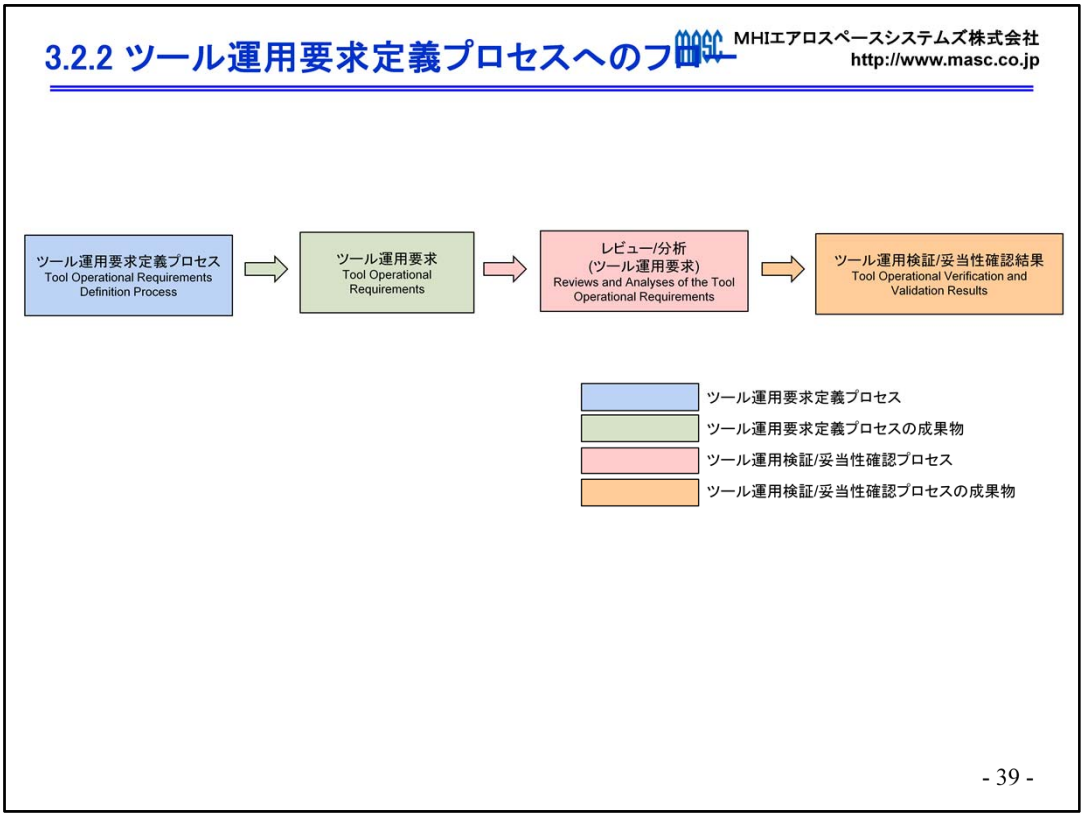


前述した通りツールの運用要求定義プロセスでは、

ソフトウェア計画とツール計画をもとにツールがどのように運用されるのかを明らかにし、それをツール運用要求にまとめる。

ツール運用要求定義プロセスの入力として、ソフトウェア計画が利用され得るのは、

ツール運用要求がかけるように、各計画書に手順が細かく定義されているからである。



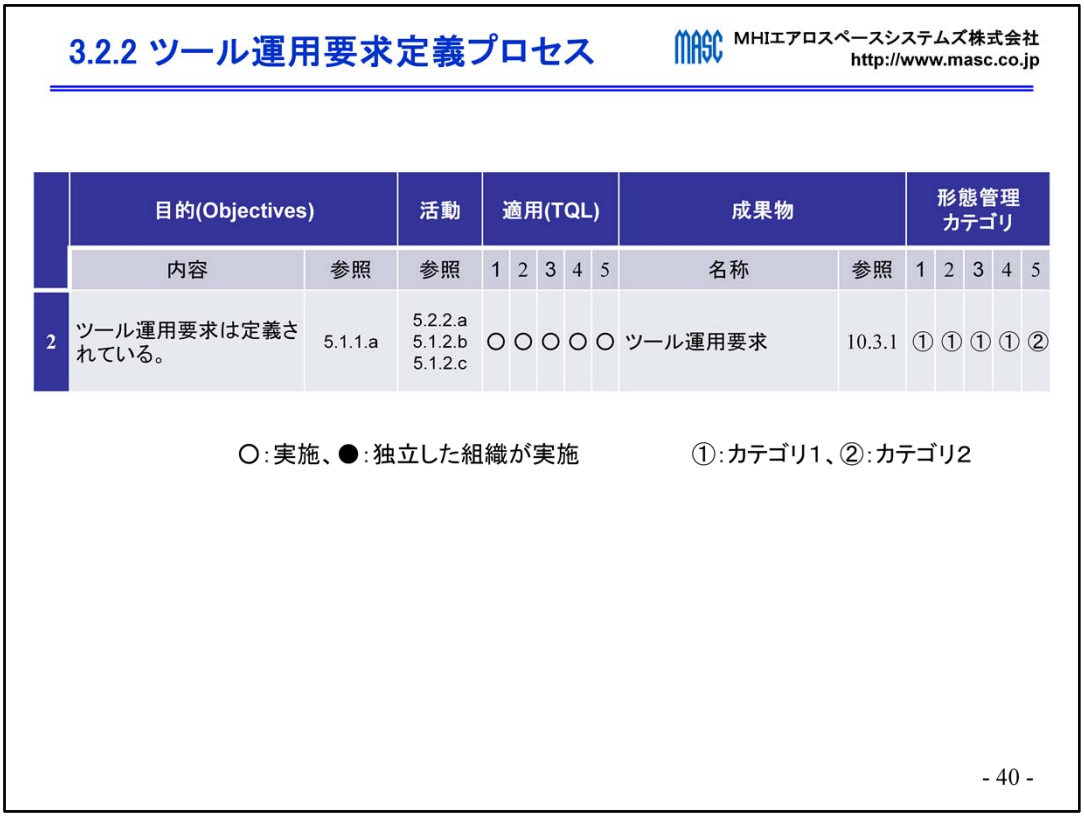
【5.2.1】

このフローはツール運用要求定義プロセスと、それに関連するツール検証/妥当性確認プロセスの関係を示している。

ツール要求定義プロセスの成果物であるール運用要求(Tool Operational Requirements)に対し、

ツール運用検証/妥当性確認プロセス(Tool Operational Verification and Validation Process)によってレビュー/分析が行われる。

レビュー/分析の結果はツール運用検証/妥当性確認結果(Tool Operational Verification and Validation Results)としてまとめられる。



3.2.2 ツール運用要求定義プロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
2	ツール運用要求は定義されている。	5.1.1.a	5.2.2.a 5.1.2.b 5.1.2.c	○	○	○	○	○	ツール運用要求	10.3.1	①	①	①	①	②

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

- 40 -

【Table T-0】

この表は、TQKごとの、ツール運用要求定義プロセスのObjectivesを示している。
ツール運用要求定義プロセスは、ツール運用要求が定義されていることを保証する。

《5.1.1》ツール運用要求の目的 (Tool Operational Requirements Definition Process)

ツール運用要求プロセスの要求は:

a. ツール運用要求が定義される。

《5.1.1》

《5.1.2》ツール運用要求の活動(Tool Operational Requirements Objectives)

このプロセスの活動には以下のものがある。

a. ツール運用要求は、セクション10.3.1で定義される全ての項目を最低限含むよう開発されなければならない。

b. ツール運用要求は検証可能で、また一貫性がなければならない。それらには、ツールの機能性及びアウトプットが、ツールにより実行される特定されたソフトウェアライフサイクルの活動と一致するということを確認するため十分な詳述がなければならない。

c. ツール運用要求は、自動化、削除、又は削減されるプロセスを満足させるための信用を取ることを正当化するツールの検証を支援するため十分な詳述を提供しなければならない。

《5.1.2》

3.2.3 レビュー/分析(ツール運用要求)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
4	ツール運用要求は完全であり、正確であり、検証可能であり、一貫している。	6.2.1.a	6.2.2.a	●	●	○	○		ツール運用検証/妥当性確認結果	10.3.4	②	②	②	②	
6	ツール運用要求は十分であり、正しい。	6.2.1.aa	6.2.2.b	●	●	○	○	○	ツール運用検証/妥当性確認結果	10.3.4	②	②	②	②	②

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

- 41 -

【Table T-0】

これはツール運用要求定義プロセスの成果物であるツール運用要求に対するレビュー／分析の活動である。
レビューのポイントは、表にあげた2項目である。

3.2.4 ツール資格データ (1/2)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

(1) ツール運用要求(Tool Operational Requirement)

ツール運用要求は、ソフトウェアライフサイクルプロセスの観点(つまり、ツールを利用するプロセス)から、ツールの機能性及びインターフェースを定義する。

ここには、以下が記載されなければならない。

- ツール使用状況(他ツールとのインターフェース、結果として生じるソフトウェアへのツール成果物の統合など)
- ツール運用環境
- 入力ファイル(フォーマット、言語定義など)
- 出力ファイル(フォーマット、コンテンツなど)
- 識別されたソフトウェアライフサイクルプロセスを満たすため使用される、全てのツール機能及び技術特徴についての要求

- 42 -

【10.3.1】

ツール運用要求プロセスの成果物はツール運用要求(Tool Operational Requirement)である。

ツール運用要求(Tool Requirement)には、ソフトウェアライフサイクルプロセスの視点(つまり、ツールを利用するプロセス)から、ツールの機能性とインターフェースを定義する。

《11.1》 ツール運用要求(Tool Operational Requirements)

ツール運用要求は、ソフトウェアライフサイクルプロセスの観点(つまり、ツールを利用するプロセス)から、ツールの機能性及びインターフェースを定義する。ツール運用要求には、便宜、下記項目がなくてはならない。

a. 他のツールとのインターフェースや、結果として生じるソフトウェアへのツール成果物(output)の統合などの、ツール使用コンテキスト(context)の記載

b. (ツールがインストールされる)ツール運用環境の記載

c. フォーマット、言語定義などの、入力ファイルの記載

d. フォーマットやコンテンツなどの、出力(output)ファイルの記載

e. 識別されたソフトウェアライフサイクルプロセスを満たすため使用される、全てのツール機能及び技術特徴についての要求

f. ツールによって検出されなければならない異常起動(abnormal activation)や矛盾した入力に対処するための要求。これらの要求は、ツールの機能性や出力によるそれらのモードの影響を考慮しなければならない(この項目はTQL-5に適用できない)。

g. ユーザーズマニュアル、インストールガイド、またそれらへのレファレンスのような、適切なユーザー情報(もし、それらがツール要求データの一部として作成されないなら)

h. ツール(選択オプション、パラメータ、変数、コマンドラインなど)の運用利用の記載

i. ツール出力(output)の振る舞いを明記するパフォーマンス要求

《11.1》

3.2.4 ツール資格データ (2/2)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

(1) ツール運用要求(Tool Operational Requirement) (続き)

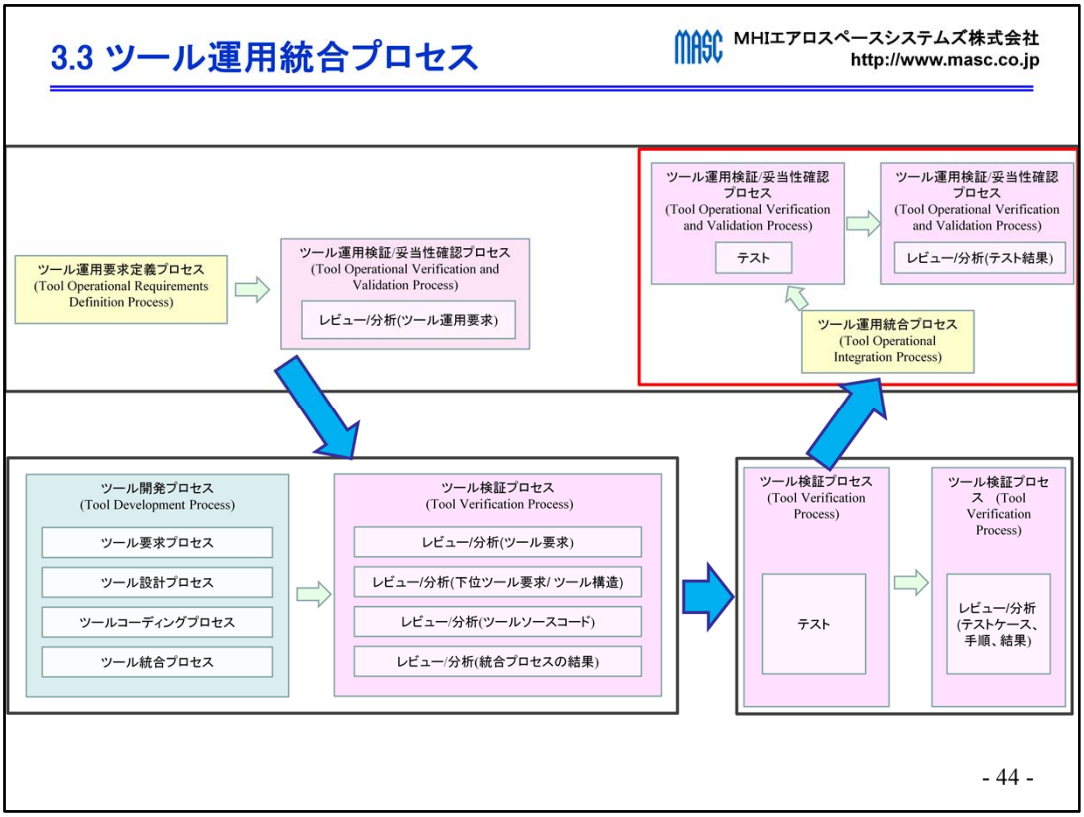
- ツールで検出されるべき異常起動(abnormal activation mode)や矛盾した入力に対処するための要求
- ユーザーマニュアル、インストールガイド、またそれらへのレファレンスのような、適切なユーザー情報(これらはツール要求の一部として作成されても良い)
- ツールの運用利用(選択オプション、パラメータ、変数、コマンドラインなど)の記載
- ツール出力の振る舞いを特定する性能要求

- 43 -

【10.3.1】

ツール運用要求プロセスの成果物はツール運用要求(Tool Operational Requirement)である。

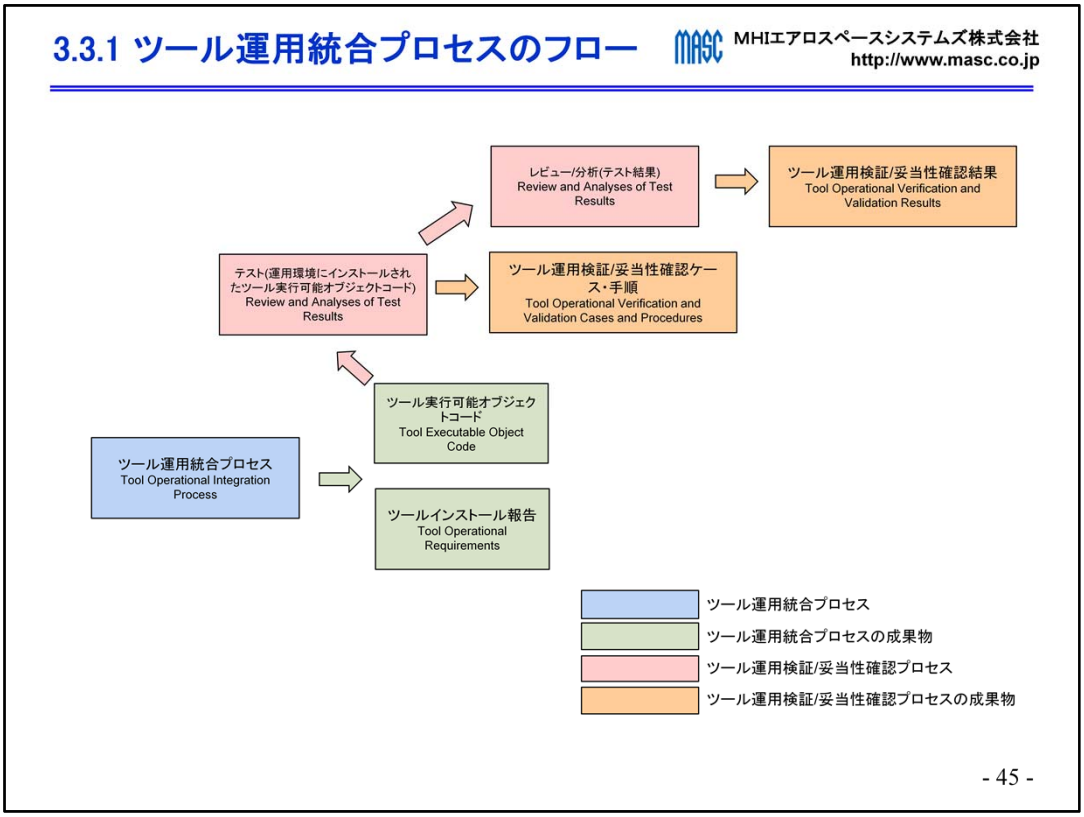
ツール運用要求(Tool Requirement)には、ソフトウェアライフサイクルプロセスの視点(つまり、ツールを利用するプロセス)から、ツールの機能性とインターフェースを定義する。



【5.3】

上流右側のツール運用統合プロセスについて説明する。
ツール運用統合プロセスは、ツールを運用環境にインストールするものである。

ツール開発プロセス(Tool Development Process)より以下をインプットとして受ける。
(a)　ユーザーマニュアル(User Manual)
(b) ツール実行可能オブジェクトコード(Tool Executable Object Code)



【5.2.1】

このフローはツール運用統合プロセスと、それに関連するツール運用検証/妥当性確認プロセスの関係を示している。

ツール運用統合プロセスの成果物は運用環境にインストールされたツール実行可能オブジェクトコード、ツールインストール報告である。

ツール運用検証/妥当性確認プロセス(Tool Operational Verification and Validation Process)では、そのツール実行オブジェクトコードを対象に、

それがツール運用要求に従うかを保証するため、テストが行われる。

また、テスト結果に対してレビュー/分析が行われる。

検証/妥当性確認の結果は、ツール運用検証/妥当性確認ケース・手順、またツール運用検証/妥当性確認結果(Tool Operational Verification and Validation Results)としてまとめられる。

3.3.2 ツール運用統合プロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
3	ツール実行可能オブジェクトコードは、ツール運用環境にインストールされている。	5.3.1.a	5.3.2.a 5.3.2.b 5.3.2.c	○	○	○	○	○	ツール実行可能オブジェクトコード	10.2.4	②	②	②	②	②
									ツールインストール報告	10.3.2	②	②	②	②	②

- 46 -

【Table T-0】

ツール運用統合プロセスは、ツール実行可能オブジェクトコーが、ツール運用環境にインストールされていることを保証するものである。

《5.3.1》ツール運用統合プロセスの目的(Tool Operational Integration Process Objectives)

ツール運用統合プロセスの目的は:

a. ツール実行可能オブジェクトコードが、ツール運用環境へインストールされる。

《5.3.1》

《5.3.2》ツール運用統合の活動(Tool Operational Integration Activities)

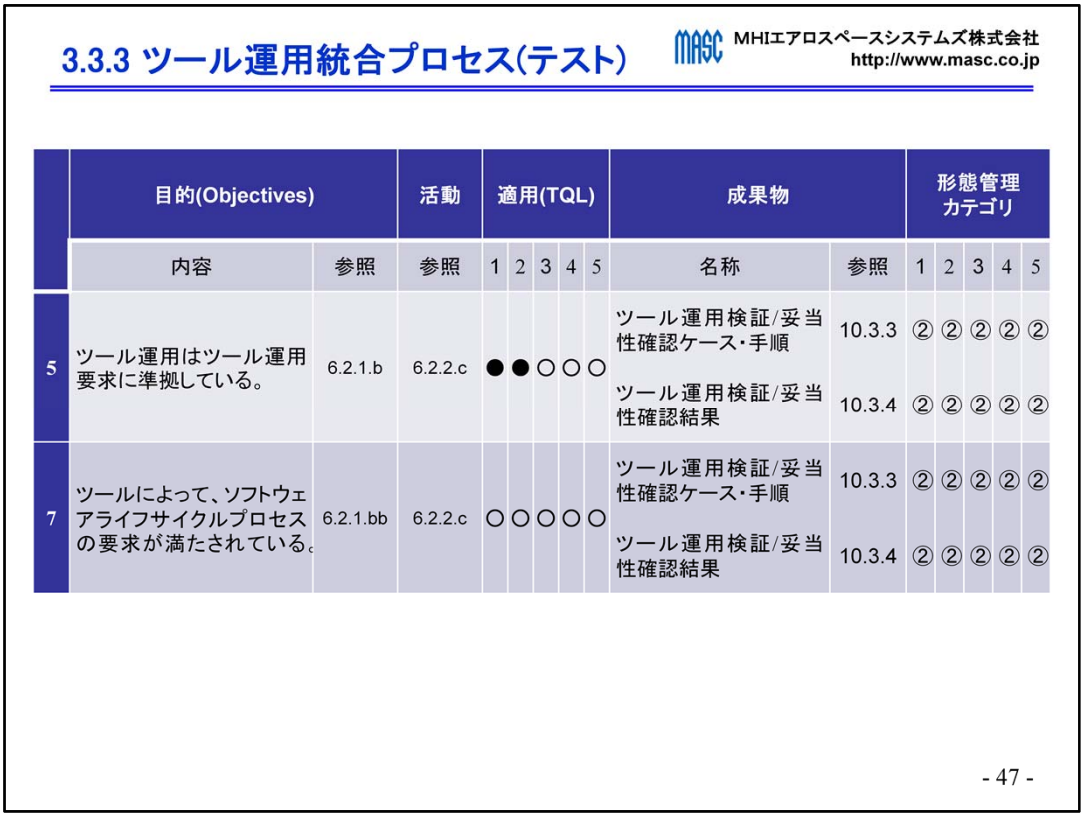
このプロセスの活動は:

a. ツール実行可能オブジェクトコード(設定ファイルのような、すべての関連ファイルを含む)は、ツール運用環境にインストールされなければならない。

b. ツール運用統合プロセスの間に検出される不十分又は誤った入力は、不十分又は誤った入力を生産したプロセスへ提供されなければならない。

c. ツールインストール報告は生成されなければならない(10.3.2を参照)。

《5.3.2》



3.3.3 ツール運用統合プロセス(テスト)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
5	ツール運用はツール運用要求に準拠している。	6.2.1.b	6.2.2.c	●	●	○	○	○	ツール運用検証/妥当性確認ケース・手順	10.3.3	②	②	②	②	②
									ツール運用検証/妥当性確認結果	10.3.4	②	②	②	②	②
7	ツールによって、ソフトウェアライフサイクルプロセスの要求が満たされている。	6.2.1.bb	6.2.2.c	○	○	○	○	○	ツール運用検証/妥当性確認ケース・手順	10.3.3	②	②	②	②	②
									ツール運用検証/妥当性確認結果	10.3.4	②	②	②	②	②

- 47 -

【Table T-0】

この表はツール検証/妥当性確認プロセスにおけるレビュー／分析に関しての規定を定めており、
ツール運用が要求に基づき行われていることを保証するものである。

5項は、ツール運用がツール運用要求に準拠していることを求めている。
7項は、ツールによってソフトウェアライフサイクルの要求が満たされていることを保証するものである。

4. ツール開発プロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

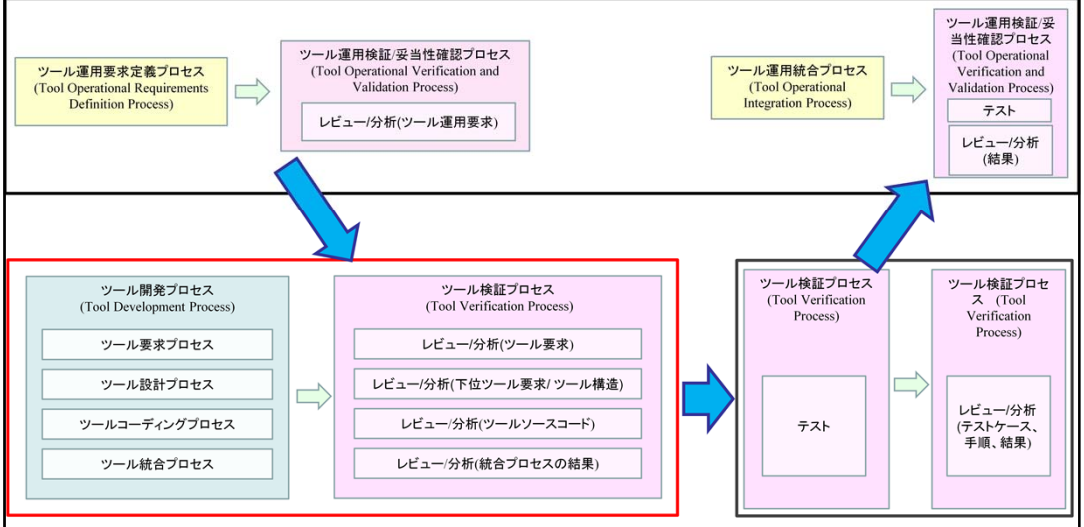
ツール開発プロセス
(Tool Development Process)

1. ツール開発プロセスのフロー
2. ツール要求プロセス
3. ツール設計プロセス
4. ツールコーディングプロセス
5. ツール統合プロセス
6. トレーサビリティ

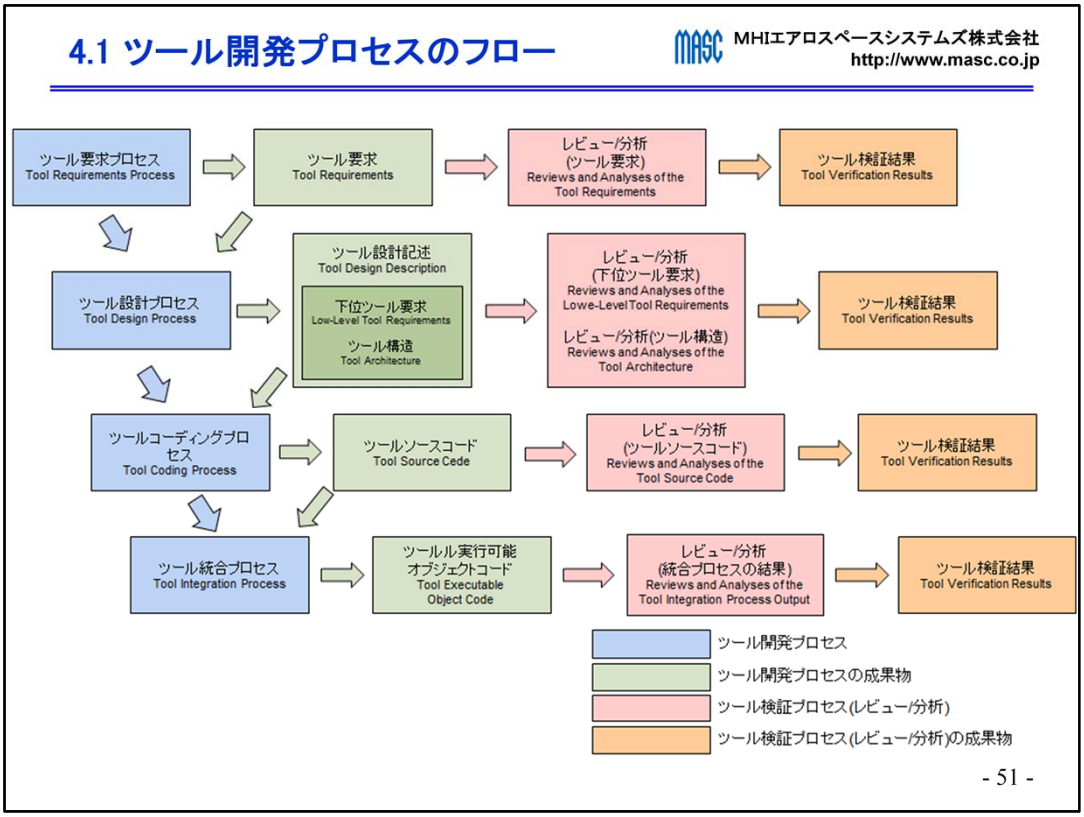
【4】

4.0 ツール開発プロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp



- 50 -



【5.2】

このフローはツールプロセスと関連するツール検証プロセスの関係を示している。

左のブルーのフローがツール開発プロセスを示し、グリーンのブロックがそのプロセスにおける成果物を示している。

中央右のピンクのブロックはツール検証プロセス内の「レビュー／分析」であり、主として成果物を対象としている（一部プロセスを対象とする）。右のオレンジのブロックは「レビュー／分析」の結果をまとめた成果物である。

以降、ツール開発プロセスの各プロセスについて説明する。

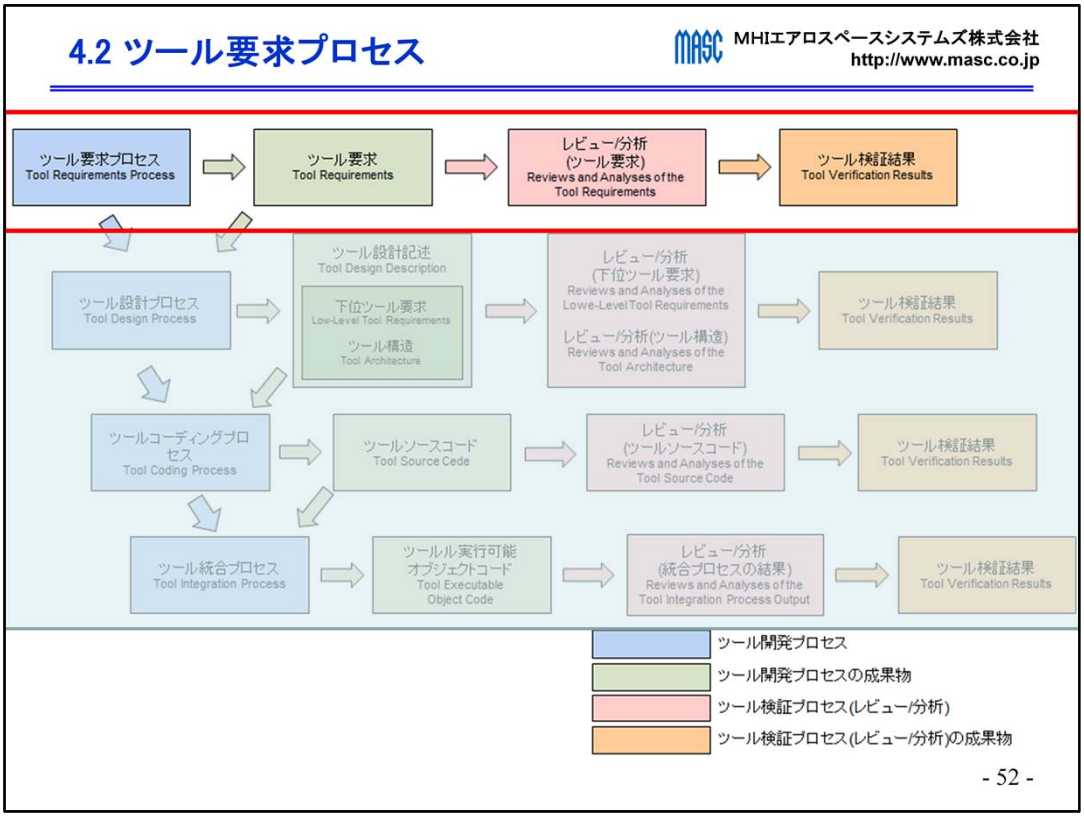
このフローにあるように、ソフトウェア開発プロセスは、ソフトウェア検証プロセスの「レビュー／分析」と並行して実施される。

従って、以降の説明においても次の順に進めることとする。

(1)各開発プロセスの説明（ブルーのブロック）

(2)レビュー／分析の説明（ピンクのブロック）

(3)成果物の説明（グリーンのブロック）



【5.2.1】

ここでは、ツール要求プロセス(Tool Requirements Process)について説明する。

ツール要求プロセスは、ツール運用要求をインプットとして、
ツール要求、また必要なら派生ツール要求を設定するものである。
これらのアウトプットは成果物として、ツール要求(Tool Requirements)にまとめられる。

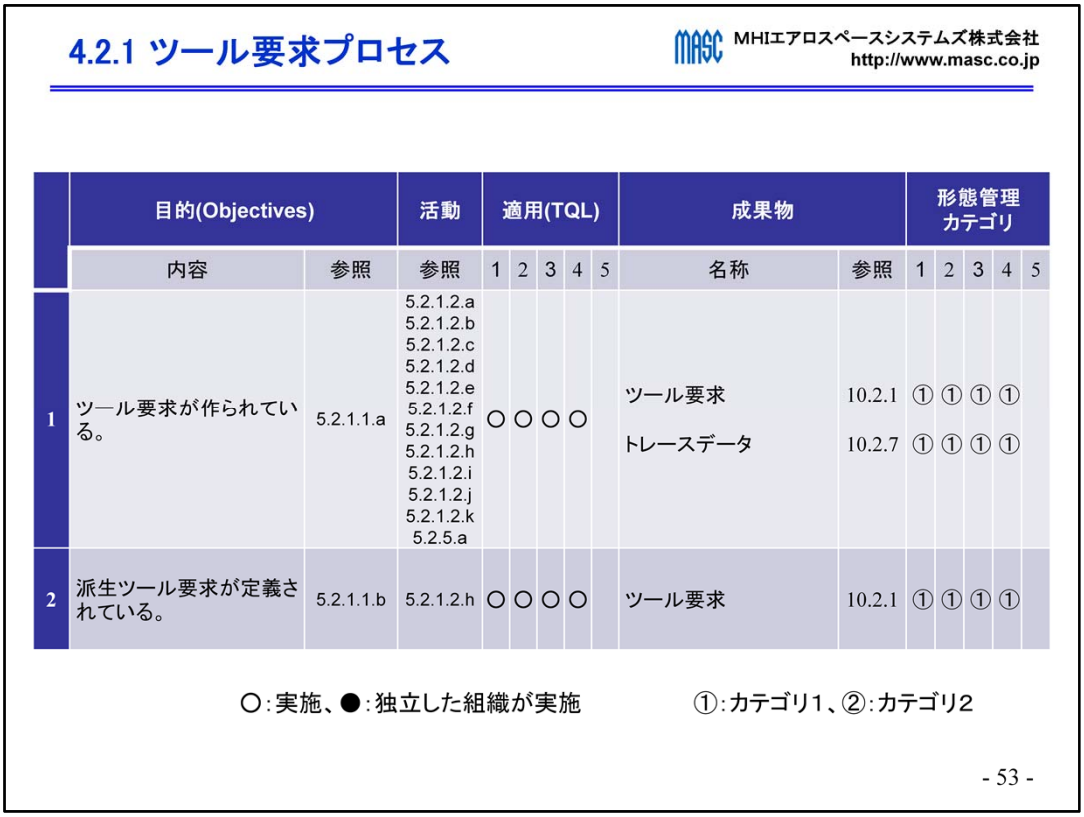
ツール運用要求定義(Tool Operational Requirements Definition Process)プロセスより以下をインプットとして受け取る。

(a) ツール運用要求(Tool Operational Requirements)

ツール資格計画プロセス(Tool Qualification Planning Process)より以下をインプットとして受け取る。

(a) ツール開発計画(Tool Development Plan)

(b) ツール要求標準(Tool Requirements Standards)



4.2.1 ツール要求プロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
1	ツール要求が作られている。	5.2.1.1.a	5.2.1.2.a 5.2.1.2.b 5.2.1.2.c 5.2.1.2.d 5.2.1.2.e 5.2.1.2.f 5.2.1.2.g 5.2.1.2.h 5.2.1.2.i 5.2.1.2.j 5.2.1.2.k 5.2.5.a	○	○	○	○		ツール要求 トレースデータ	10.2.1 10.2.7	① ①	① ①	① ①	① ①	
2	派生ツール要求が定義されている。	5.2.1.1.b	5.2.1.2.h	○	○	○	○		ツール要求	10.2.1	①	①	①	①	

○：実施、●：独立した組織が実施　　①：カテゴリ1、②：カテゴリ2

- 53 -

【Table T-2】

ツール要求プロセスで生成されるツール要求は、世間一般で言われるところのツールの機能仕様と捉えて良い。

DO-330では、あくまでもこのプロセスのインプットであるツール運用要求を基本として、必ず双方向にトレースがとれていることを求めている。派生ツール要求(Derived Tool Requirements)は、ツール運用要求とトレースができない要求であり、このプロセスで新たに発生した要求のことである。派生ツール要求は、その存在が正当化され、それらがツール運用要求で定義された期待される機能と成果物に影響を与えないことを確かめるため評価されなければならない。

《5.2.1.1》ツール要求の目的(Tool Requirements Activities)

ツール要求プロセスの目的は:

a. ツール要求が作成される。
b. 必要なら、派生ツール要求が定義される。

《5.2.1.1》
《5.2.1.2》ツール要求(Tool Requirements Activities)

このプロセスの活動は:

a. ツール要求が作成され、また、ツールがツール運用要求を満たすかどうか、決定する方法で、文書で確認しなければならない。
b. ツール要求には、ツールに実現される全ての機能及びインターフェース関連の要求が含まれなければならない。
c. ツール要求は、ツール開発計画で述べられるプロセスの後で作成されなければならない。
d. ツール要求はツール要求標準を利用して作成されなければならない。

e. ル要求は検証可能で一貫性がなければならない。

f. ツール要求は、異常行動が検出され、無効な結果が予防されるように定義されなければならない。例えば、ツールにとって誤った結果を生じるよりは、結果を生じないほうが良い。それ故、ツール要求は故障モードについて述べ、故障条件への応答を記述しなければならない。

g. 各ツール要求は、派生ツール要求を除き、1つ以上のツール運用要求へトレースしなければならない。

h. 派生ツール要求は、ツール運用要求へトレース可能ではない要求である。派生ツール要求の存在は正当化され、それらがツール運用要求で定義された機能と成果物に負の影響を与えないことを確かにするために評価されなければならない。

i. ツール要求には、取り扱い説明書、エラーメッセージのリスト、及び制限が記載されなければならない。

j. ツール要求は、ツール運用要求にトレースしない未使用ツール機能に関係した要求を明確にしなければならない。マルチファンクションツールのガイダンスについてはセクション11.1を参照せよ。

k. ツール要求は、適切な実現を確かにするため、またツール(例えば、基礎となるモデル又は数学的理論)の正当性を評価するため、適切な詳細のレベルで定義されなければならない。

《5.2.1.2》

4.2.2 レビュー/分析(ツール要求)（1/2）

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
1	ツール要求はツール運用要求を順守している。	6.1.3.1.a	6.1.3.1	●	●	○	○		ツール検証結果	10.2.6	②	②	②	②	
2	ツール要求は正確であり、一貫している。	6.1.3.1.b	6.1.3.1	●	●	○	○		ツール検証結果	10.2.6	②	②	②	②	
3	ツール運用環境との整合に関する要求が定義されている。	6.1.3.1.c	6.1.3.1	●	●	○	○		ツール検証結果	10.2.6	②	②	②	②	
4	ツール要求はエラー条件に応じて振る舞いを定義している。	6.1.3.1.d	6.1.3.1	●	●	○	○		ツール検証結果	10.2.6	②	②	②	②	

○：実施、●：独立した組織が実施　　①：カテゴリ1、②：カテゴリ2

- 54 -

【6.1.3.1】

ここではツール要求プロセスの成果物であるツール要求（具体的にはソフトウェア上位要求）に対するレビュー／分析について説明する。レビューのポイントは、次のスライドも含め、表に挙げた9項目である。7項目のみがソフトウェア要求プロセスそのものに対するレビューである。

《6.1.3.1》ツール要求のレビュー/分析(Reviews and Analyses of the Tool Requirements)

これらのレビュー/分析の目的はツール要求プロセスで入り込んだエラーを検出し、報告することである。これらのレビュー/分析の活動はツール要求が以下の目的を満たすことを確かにする。

a. ツール運用要求への準拠：目的は全てのツール運用要求がツール要求へ実現され、派生ツール要求及びそれらの存在理由が正しく定義されることを保証することである。

b. 正確性と一貫性：目的は、各ツール要求が正確で、明確で、そして十分に詳しいこと、また要求がお互いに矛盾しないことを保証することである。この目的には、適切な実現を保証するため、またツールの正しさを評価するため、ツール要求の詳細さのレベルが適切であるという検証がある。

c. ツール運用環境の互換性：目的は、ツール運用環境との互換性に対処するための制約が存在する場合、互換性要求が定義されることを保証することである。

d. 故障モードとエラー：目的は、ツール要求が故障モードに対応するエラー条件及び特有の要求に応じてツールの振る舞いを定義すること、また不正確な入力を識別することを保証することである。

e. ユーザ情報：目的は、ツール要求がユーザ取り扱い説明書(user instructions)、エラーメッセージリスト、及び制約を提供すること保証することである。

f. 検証可能性：目的は、ツール要求が検証可能であることを保証することである。

g. 標準への準拠: 目的は、ツール要求プロセスの間ツール要求標準に従い、標準からの逸脱が正当化されたことを保証することである。

h. トレーサビリティ: 目的は、ツール運用要求がツール要求へ落とし込まれたことを保証することである。

i. アルゴリズム: 目的は、特に不連続領域において、提案されたアルゴリズムの正確さと振る舞いを保証することである。

《6.1.3.1》

4.2.2 レビュー/分析(ツール要求) (2/2)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
5	ツール要求はユーザー取り扱い説明書及びエラーメッセージを定義している。	6.1.3.1.e	6.1.3.1	●	●	○	○		ツール検証結果	10.2.6	②	②	②	②	
6	ツール要求は検証可能である。	6.1.3.1.f	6.1.3.1	○	○	○	○		ツール検証結果	10.2.6	②	②	②	②	
7	ツール要求はツール要求標準に準拠している。	6.1.3.1.g	6.1.3.1	○	○	○			ツール検証結果	10.2.6	②	②	②		
8	ツール要求はツール運用要求へトレース可能である。	6.1.3.1.h	6.1.3.1	○	○	○	○		ツール検証結果	10.2.6	②	②	②	②	
9	アルゴリズムが正確である。	6.1.3.1.i	6.1.3.1	●	●	○	○		ツール検証結果	10.2.6	②	②	②	②	

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

【6.1.3.1】

《6.1.3.1》ツール要求のレビュー/分析(Reviews and Analyses of the Tool Requirements)

これらのレビュー/分析の目的はツール要求プロセスで入り込んだエラーを検出し、報告することである。これらのレビュー/分析の活動はツール要求が以下の目的を満たすことを確かにする。

a. ツール運用要求への準拠: 目的は全てのツール運用要求がツール要求へ実現され、派生ツール要求及びそれらの存在理由が正しく定義されることを保証することである。

b. 正確性と一貫性: 目的は、各ツール要求が正確で、明確で、そして十分に詳しいこと、また要求がお互いに矛盾しないことを保証することである。この目的には、適切な実現を保証するため、またツールの正しさを評価するため、ツール要求の詳細さのレベルが適切であるという検証がある。

c. ツール運用環境の互換性: 目的は、ツール運用環境との互換性に対処するための制約が存在する場合、互換性要求が定義されることを保証することである。

d. 故障モードとエラー: 目的は、ツール要求が故障モードに対応するエラー条件及び特有の要求に応じてツールの振る舞いを定義すること、また不正確な入力を識別することを保証することである。

e. ユーザ情報: 目的は、ツール要求がユーザ取り扱い説明書(user instructions)、エラーメッセージリスト、及び制約を提供すること保証することである。

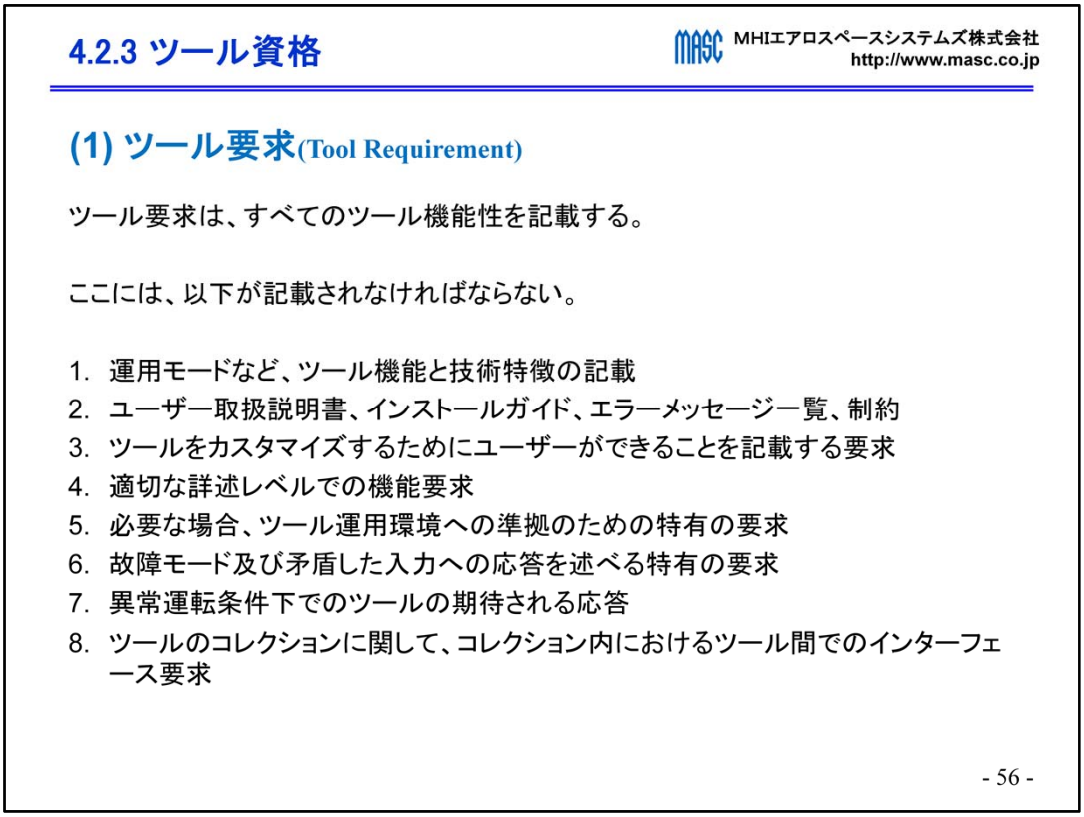
f. 検証可能性: 目的は、ツール要求が検証可能であることを保証することである。

g. 標準への準拠: 目的は、ツール要求プロセスの間ツール要求標準に従い、標準からの逸脱が正当化されたことを保証することである。

h. トレーサビリティ: 目的は、ツール運用要求がツール要求へ落とし込まれたことを保証することである。

i. アルゴリズム: 目的は、特に不連続領域において、提案されたアルゴリズムの正確さと振る舞いを保証することである。

《6.1.3.1》



【10.2.1】

ツール要求プロセスの成果物はツール要求(Tool Requirement)である。
ツール要求(Tool Requirement)には、すべてのツール機能性を定義する。

《10.2.1》ツール要求(Tool Requirements)

ツール要求は、すべてのツールの機能性を記載する。このデータは以下を含まなければならない。

a. 運用モードなど、ツール機能と技術特徴の記載

b. 取扱説明書(user instructions)、インストールガイド(installation instructions)、エラーメッセージ一覧、そして制約事項。しばしばこれは、ユーザーズマニュアルとしてまとめられる。このユーザーズマニュアルはツール要求の一部であっても良いし、1つ以上の資料にまとめられてもよい。

c. ツールをカスタマイズするためにユーザーができることを記載する要求

d. 適切な詳述レベルでの機能要求(5.2.1.2.kを参照せよ)

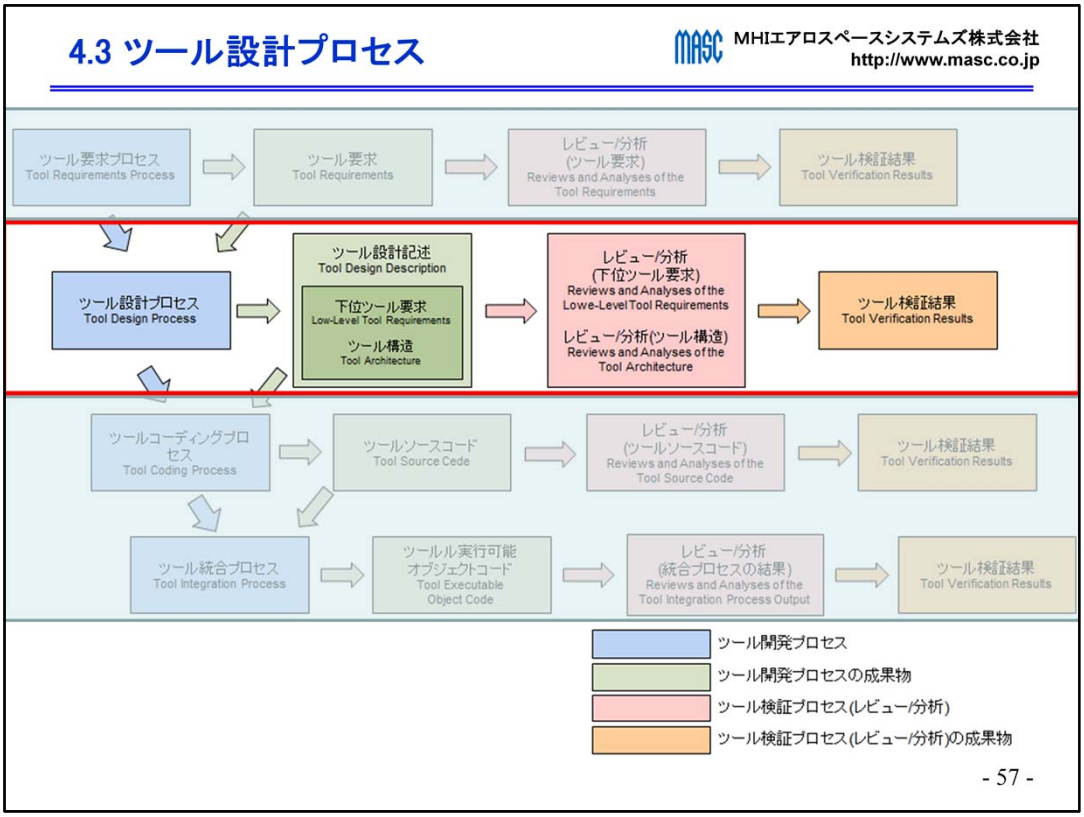
e. もし必要なら、ツール運用環境への準拠のための特有の要求

f. 故障モード及び矛盾した入力への応答を述べる特有の要求

g. 異常運転条件下でのツールの期待される応答

h. ツールのコレクション(collection)に関して、コレクション(collection)内におけるツール間でのインターフェース要求

《10.2.1》



【5.2.2】

ここでは、ツール設計プロセス(Tool Design Process)について説明する。

ツール設計プロセスは、ツール要求(Tool Requirements)からツール構造(Tool Architecture)と下位ツール要求(Low-Level Tool Requirements)、及び派生下位ツール要求(Derived Low-Level Tool Requirements)を設定するものである。これらのアウトプットは成果物としてツール設計記述(Tool Design Description)にまとめられる。

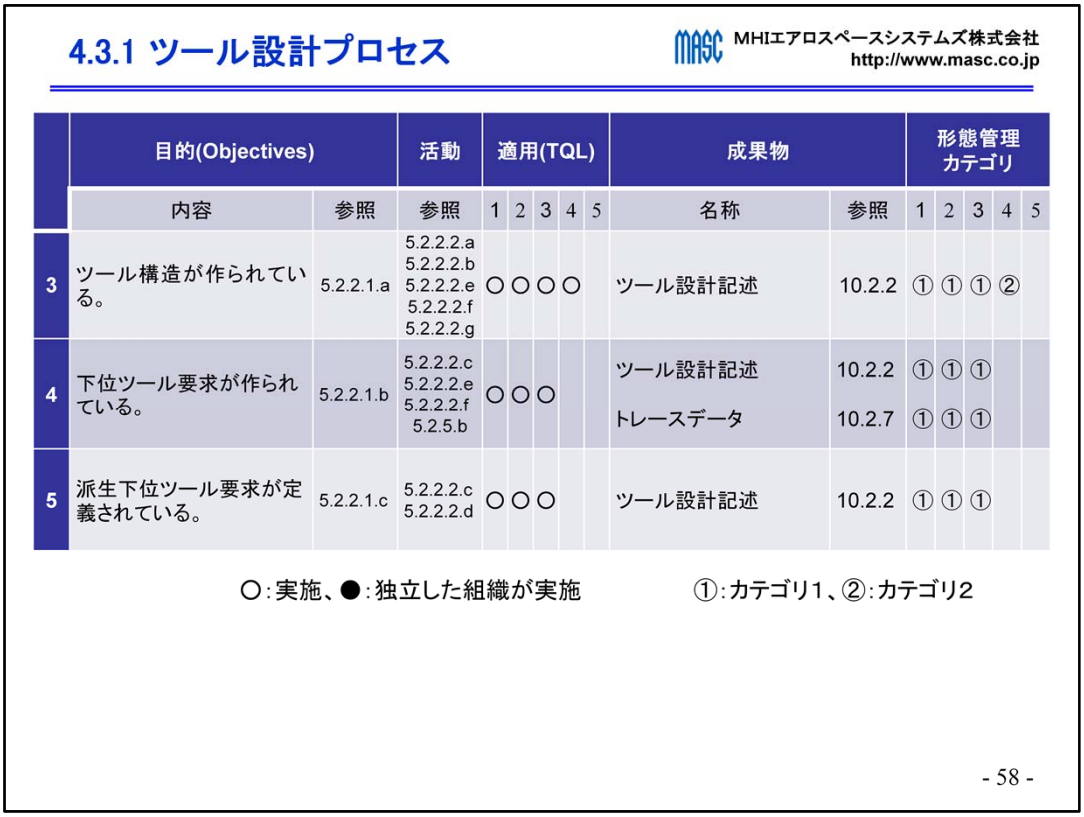
ツール要求プロセス(Tool Requirements Process)より以下をインプットとして受ける。

(a) ツール要求データ(Tool Requirements)

ツール資格計画プロセス(Tool Qualification Planning Process)より以下をインプットとして受け取る。

(a) ツール開発計画(Tool Development Plan)

(b) ツール設計標準(Tool Design Standards)



4.3.1 ツール設計プロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
3	ツール構造が作られている。	5.2.2.1.a	5.2.2.2.a 5.2.2.2.b 5.2.2.2.e 5.2.2.2.f 5.2.2.2.g	○	○	○	○		ツール設計記述	10.2.2	①	①	①	②	
4	下位ツール要求が作られている。	5.2.2.1.b	5.2.2.2.c 5.2.2.2.e 5.2.2.2.f 5.2.5.b	○	○	○			ツール設計記述 トレースデータ	10.2.2 10.2.7	① ①	① ①	① ①		
5	派生下位ツール要求が定義されている。	5.2.2.1.c	5.2.2.2.c 5.2.2.2.d	○	○	○			ツール設計記述	10.2.2	①	①	①		

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

- 58 -

【Table T-2】

ツール設計プロセスは、世間一般で言うところの構造設計と詳細設計がひとつになったものと言える。

DO-330では、設計の結果としてツール構造(Tool Architecture)と下位ツール要求(Low-Level Tool Requirements)の2つを挙げている。

ツール構造は、ソフトウェア間の相互作用を影響を規定した文書と言える。

後述するが、下位ツール要求はソースコードとのトレーサビリティを取る必要があるため、かなり粒度の細かいレベルでの記述を求めている。

《5.2.2.1》ツール設計の目的(Tool Design Objectives)

ツール設計記述はツール設計プロセスの間に作成される。

目的は:

a. ツール構造が作成される。
b. 下位ツール要求が作成される。
c. もし必要なら、派生下位ツール要求が定義される。

《5.2.2.2》ツール設計の活動(Tool Design Activities)

プロセスの活動は:

a. ツール設計プロセスは、ツール構造を定義しなければならない。

b. もし該当すれば、ツール設計は、保護のような全てのツール構造特徴を述べなければならない。保護は、資格(qualification)の異なるアプローチやレベルを適用するため、ツールの一部分やツールのコレクションを隔離するため使っても良い。マルチファンクションツールに関してはセクション11.1を参照すること。

c. ツール要求は、ツール要求へトレース可能である下位ツール要求に洗練されなければならないか、又は派生下位ツール要求として識別されなければならない。

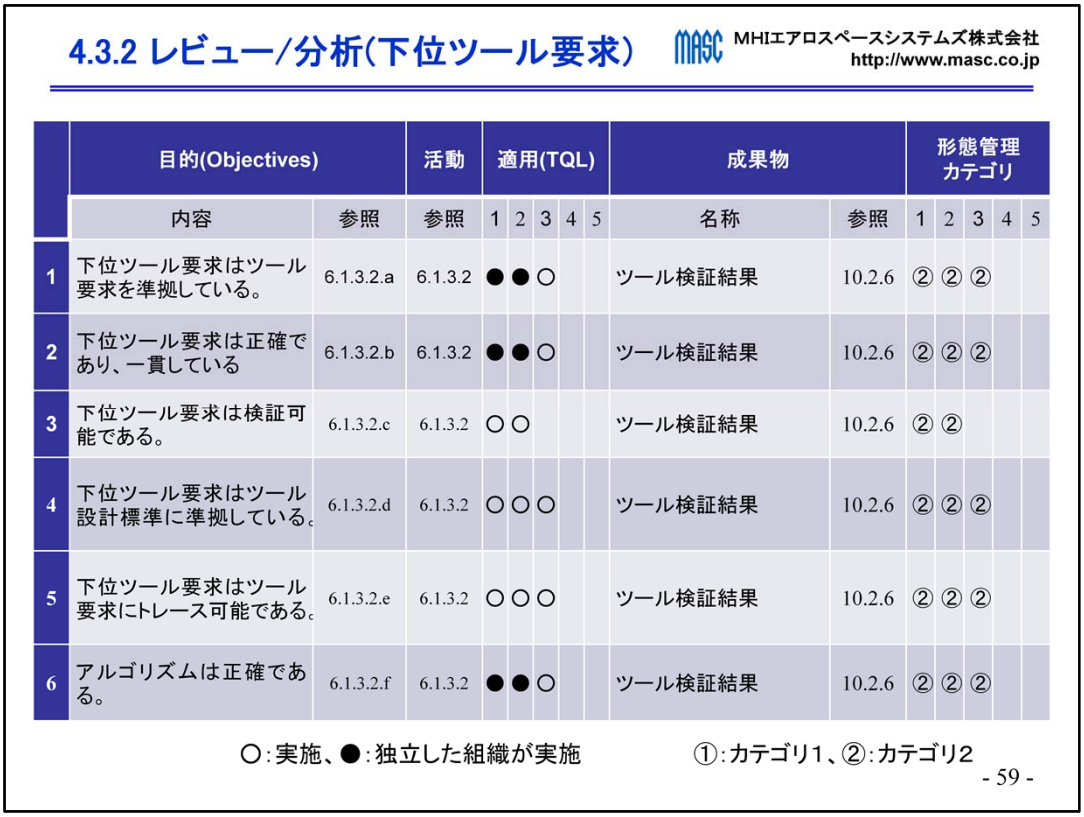
d. 派生下位ツール要求は、ツール要求へトレース可能ではない。派生要求の存在は正当化され、それらがツール運用要求で定義された期待される機能と成果物に影響を与えないことを確かめるため評価されなければならない。

e. ツール構造と下位ツール要求を含むツール設計記述は、ツール設計標準に準拠しなければならない。

f. ツール設計は検証可能で一貫性がなければならない。

g. ツールにより外部コンポーネント(ツール開発者の管理下ではない(オペレーティング・システムや外部ソフトウェア・ライブラリのような))が使用される場合、ツールにより使用されるこれらの外部コンポーネントへのインターフェースはツール設計記述で明らかにされなければならない。インターフェースの記述は、ファイル管理ルーチン、プリミティブ(primitives) 、メモリ割り当てコール、そしてユーザインターフェースを支援しているルーチン(例えば、コマンドラインやディスプレイメッセージ)のような、すべての外部コンポーネントを明らかにしなければならない。

《5.2.2.2》



4.3.2 レビュー/分析(下位ツール要求)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
1	下位ツール要求はツール要求を準拠している。	6.1.3.2.a	6.1.3.2	●	●	○			ツール検証結果	10.2.6	②	②	②		
2	下位ツール要求は正確であり、一貫している	6.1.3.2.b	6.1.3.2	●	●	○			ツール検証結果	10.2.6	②	②	②		
3	下位ツール要求は検証可能である。	6.1.3.2.c	6.1.3.2	○	○				ツール検証結果	10.2.6	②	②			
4	下位ツール要求はツール設計標準に準拠している。	6.1.3.2.d	6.1.3.2	○	○	○			ツール検証結果	10.2.6	②	②	②		
5	下位ツール要求はツール要求にトレース可能である。	6.1.3.2.e	6.1.3.2	○	○	○			ツール検証結果	10.2.6	②	②	②		
6	アルゴリズムは正確である。	6.1.3.2.f	6.1.3.2	●	●	○			ツール検証結果	10.2.6	②	②	②		

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

- 59 -

【Table T-4】

ここではツール設計プロセスの成果物のひとつである下位要求に対するレビュー／分析について説明する。レビューのポイントは表に挙げた6項目である。4項のみがツール設計プロセスそのものに対するレビューである。

《6.1.3.2》下位ツール要求のレビュー/分析 (Reviews and Analyses of the Low-Level Tool Requirements)

これらのレビュー/分析の目的はツール設計記述で入り込んだエラーを検出し、報告することである。これらのレビュー/分析の活動は下位ツール要求が以下の目的を満たすことを確認する。

a. ツール要求への準拠: 目的は、下位ツール要求がツール要求を満足させ、更に派生下位ツール要求とその存在の設計基準が正しく定義されていることを保証すことである。

b. 正確性と一貫性: 目的は、各下位ツール要求が正確で明確であること、また下位ツール要求がお互いに矛盾しないことを保証することである。

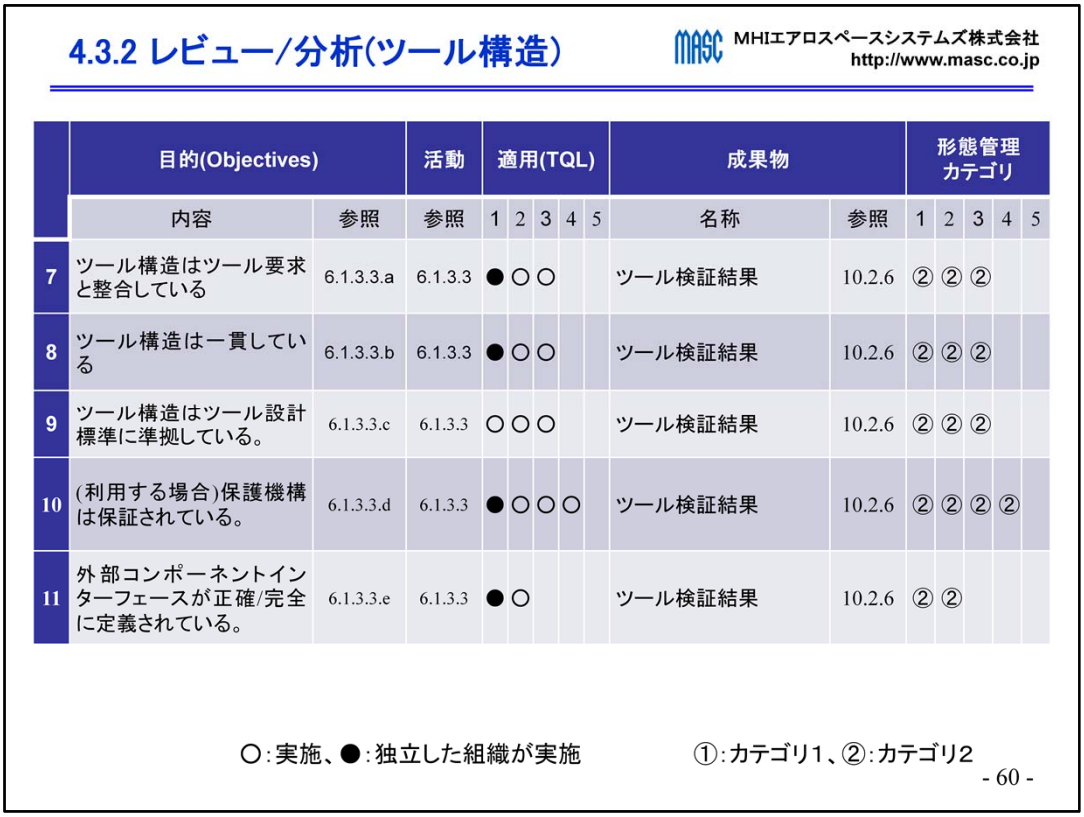
c. 検証可能性: 目的は、各下位ツール要求が検証可能であることを保証することである。

d. 標準への準拠: 目的は、適用可能な標準(TQPとツール開発計画で定義されたようにツール設計標準及び(又は)ツール要求標準)がツール設計プロセスの間ずっと適用され続けたこと、また標準からの逸脱が正当化されることを保証することである。

e. トレーサビリティ: 目的は、ツール要求及び派生ツール要求が下位ツール要求に落とし込まれたことを保証することである。

f. アルゴリズム: 目的は、特に不連続領域において、提案されたアルゴリズムの正確さと振る舞いを保証することである。

《6.1.3.2》



4.3.2 レビュー/分析(ツール構造)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
7	ツール構造はツール要求と整合している	6.1.3.3.a	6.1.3.3	●	○	○			ツール検証結果	10.2.6	②	②	②		
8	ツール構造は一貫している	6.1.3.3.b	6.1.3.3	●	○	○			ツール検証結果	10.2.6	②	②	②		
9	ツール構造はツール設計標準に準拠している。	6.1.3.3.c	6.1.3.3	○	○	○			ツール検証結果	10.2.6	②	②	②		
10	(利用する場合)保護機構は保証されている。	6.1.3.3.d	6.1.3.3	●	○	○	○		ツール検証結果	10.2.6	②	②	②	②	
11	外部コンポーネントインターフェースが正確/完全に定義されている。	6.1.3.3.e	6.1.3.3	●	○				ツール検証結果	10.2.6	②	②			

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

- 60 -

【Table T-4】

ここではツール設計プロセスのもうひとつの成果物であるツール構造に対するレビュー／分析について説明する。レビューのポイントは表に挙げた5項目である。

《6.1.3.3》ツール構造のレビュー/分析 (Reviews and Analyses of the Tool Architecture)

これらのレビュー/分析の目的はツール構造の開発で入り込んだエラーを検出し、報告することである。これらのレビュー/分析の活動はツール構造が以下の目的を満たすことを確認する。

a. ツール要求の互換性: 目的は、ツール構造がツール要求と矛盾しないことを保証することである。

b. 一貫性: 目的は、ツール構造のコンポーネント間で正しい関係が存在することを保証することである。この関係はデータフロー及びコントロールフローによって存在する。

c. 標準への準拠: 目的は、ツール設計プロセスの間中ずっとツール設計標準に従い、標準からの逸脱が正当化されることを保証することである。

d. 保護: 目的は、もし保護機構がツール構造の内部で利用された場合、保護違反が予防され又は隔離されることを保証することである。マルチファンクションツールに関しては11.1を参照すること。

e. 外部コンポーネントのインターフェース: 目的は、ツールと外部コンポーネントのインターフェースが正しく、且つ完全に定義されること(5.2.2.2.gを参照)を保証することである。

《6.1.3.3》

4.3.3 ツール資格データ (1/2)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

(1) ツール設計記述(Tool Design Description)

ツール設計記述は、ツール要求(Tool Requirements)を洗練するツール構造(Tool Architecture)と下位ツール要求(Low-Level Tool Requirements)の定義である。

ここでは、以下が記載されなければならない。

- 要求を実現するためのツール構成(tool structure)を定義しているツール構造(tool architecture)の記述
- どのようにツール要求がツール構造へ全て割り当てられているかの詳細な記述
- 内部と外部の両方のソフトウェア構造全体の入力/出力の記載(例えば、データ・ディクショナリ)
- 設計のデータフロー及び制御フロー
- スケジューリング手続き

- 61 -

【10.2.2】

本プロセスの成果物はツール設計記述(Tool Design Description)である。

ツール設計記述(Tool Design Description)には、ツール要求(Tool Requirements)を洗練するツール構造(Tool Architecture)と下位ツール要求(Low-Level Tool Requirements)を定義する。

《10.2.2》ツール設計記述 (Tool Design Description)

ツール設計記述は、ツール要求を洗練するツール構造と下位ツール要求の定義である。このデータは以下の項目を含まなければならない。

a. 要求を実現するためのツール構成(tool structure)を定義しているツール構造(tool architecture)の記述

b. どのようにツール要求がツール構造へ全て割り当てられているかの詳細な記述

c. 内部と外部の両方のソフトウェア構造全体の入力/出力の記述(例えば、データ・ディクショナリ)

d. 設計のデータフロー及び制御フロー

e. スケジューリング手続き

f. もし利用されるなら、保護

g. ソフトウェアコンポーネント、それは新しく開発された又は以前に開発されていたのか、また以前に開発されたものの場合、それらが取られるベースラインへの参照についての記載

h. ツール要求を実現し、またそれへトレース可能な下位ツール要求

i. ツール設計プロセスに起因する派生下位ツール要求

《10.2.2》

4.3.3 ツール資格データ (2/2)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

(1) ツール設計記述(Tool Design Description)　(続き)

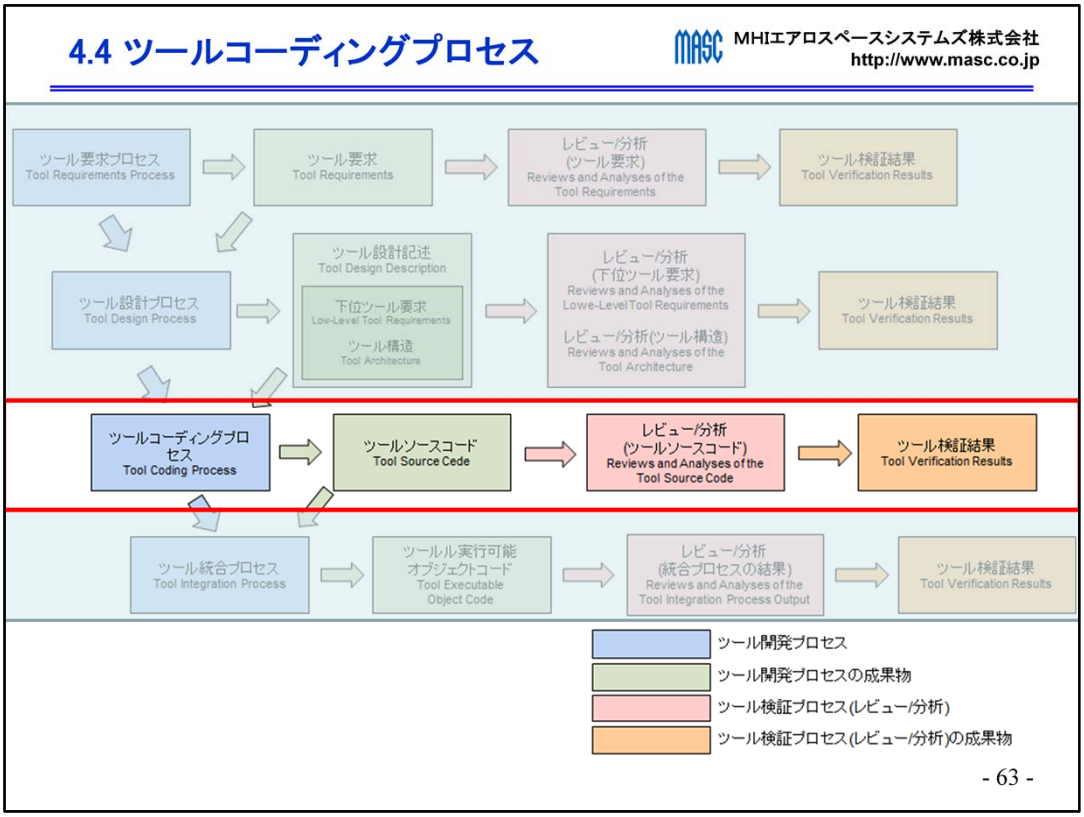
- 使用される場合の保護
- ソフトウェアコンポーネントの記載 (新開発か既開発か。既開発の場合、それらが取られたベースラインへの参照についての記載)
- ツール要求を実現し、またそれへトレース可能な下位ツール要求
- ツール設計プロセスに起因する派生下位ツール要求

- 62 -

【10.2.2】

本プロセスの成果物はツール設計記述(Tool Design Description)である。

ツール設計記述(Tool Design Description)には、ツール要求(Tool Requirements)を洗練するツール構造(Tool Architecture)と下位ツール要求(Low-Level Tool Requirements)を定義する。



【5.2.3】

ここでは、ツールコーディングプロセス(Tool Coding Process)について説明する。

ソフトウェアコーディングプロセスにおいては、ツール構造(Software Architecture)と下位ツール要求(Low-Level Tool Requirements)からツールソースコード(Tool Source Code)が実装される。ソースコードはトレース・検証が可能であり、一貫性があり、正しく下位ツール要求を実装しなければならない。

ツール設計プロセス(Tool Design Process)より以下をインプットとして受ける。

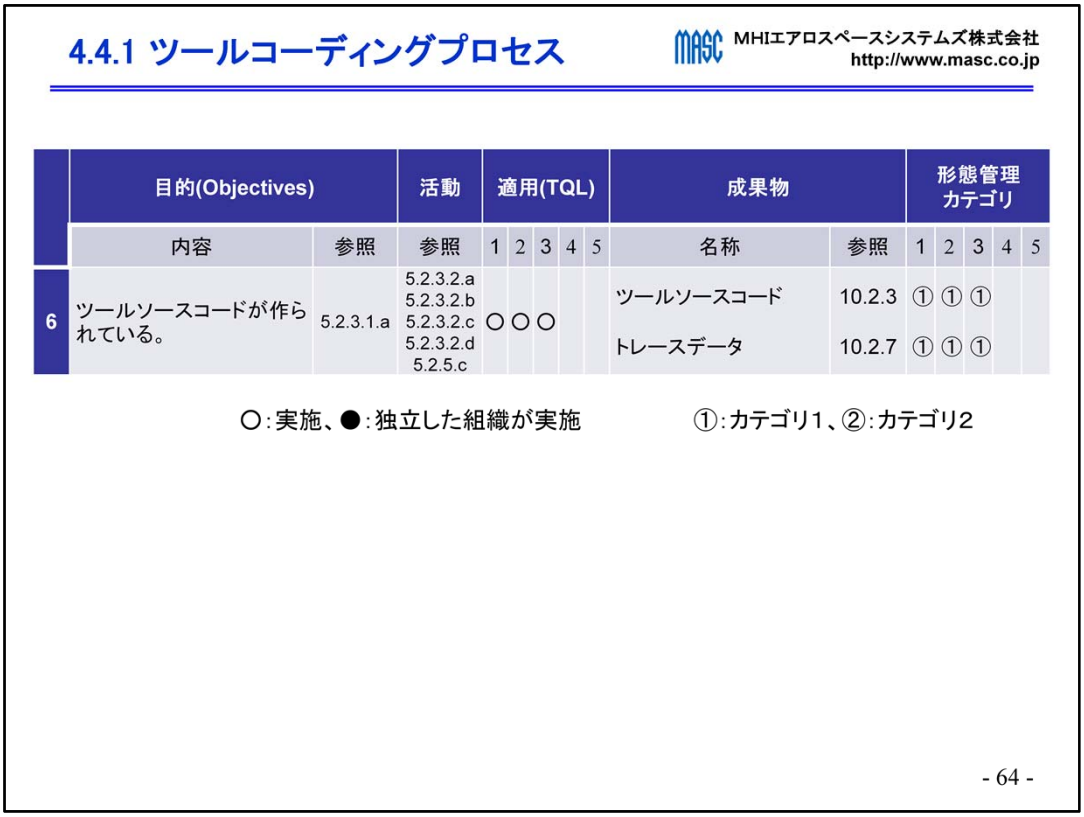
(a) 下位レベルツール要求(Low-Level Tool Requirements)

(b) ツール構造(Tool Architecture)

ツール資格計画プロセス(Tool Qualification Planning Process)より以下をインプットとして受ける。

(a) ツール開発計画(Tool Development Plan)

(b) ツールコーディング標準(Tool Code Standards)



4.4.1 ツールコーディングプロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
6	ツールソースコードが作られている。	5.2.3.1.a	5.2.3.2.a 5.2.3.2.b 5.2.3.2.c 5.2.3.2.d 5.2.5.c	○	○	○			ツールソースコード トレースデータ	10.2.3 10.2.7	① ①	① ①	① ①		

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

- 64 -

【Table T-2】

《5.2.3.1》ツールコーディングの目的(Tool Coding Process)

ツールコーディングプロセスの目的は:

a. ツールソースコードが下位ツール要求から作成される。

《5.2.3.1》

《5.2.3.2》ツールコーディングの活動(Tool Coding Activities)

このプロセスの活動は:

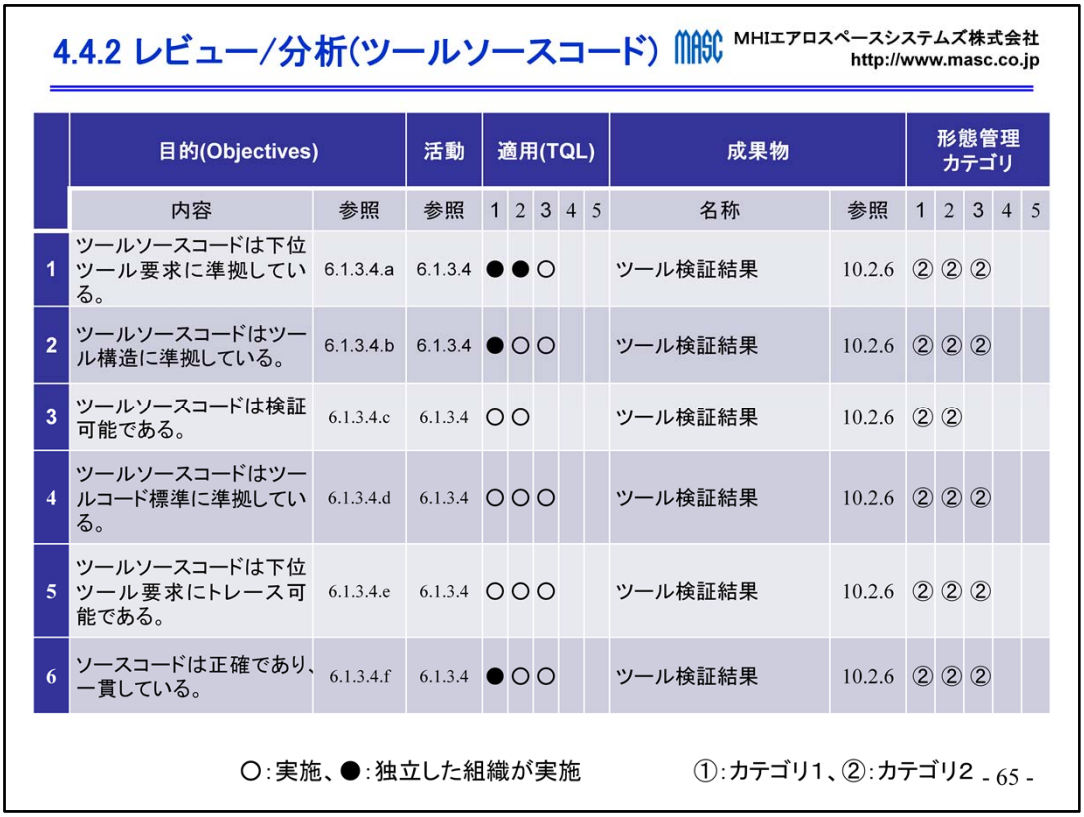
a. ツールソースコードは下位ツール要求を実現し、ツール構造に準拠しなければならない。

b. ツールソースコードはツールコード標準に準拠しなければならない。

c. ツールソースコードは下位ツール要求へトレース可能でなければならない。

d. ツールコーディングプロセスの間に検出される不十分な、又は誤った入力は、解明や修正のために誤った入力を生産したプロセスへ提供されなければならない。

《5.2.3.2》



4.4.2 レビュー/分析(ツールソースコード)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
1	ツールソースコードは下位ツール要求に準拠している。	6.1.3.4.a	6.1.3.4	●	●	○			ツール検証結果	10.2.6	②	②	②		
2	ツールソースコードはツール構造に準拠している。	6.1.3.4.b	6.1.3.4	●	○	○			ツール検証結果	10.2.6	②	②	②		
3	ツールソースコードは検証可能である。	6.1.3.4.c	6.1.3.4	○	○				ツール検証結果	10.2.6	②	②			
4	ツールソースコードはツールコード標準に準拠している。	6.1.3.4.d	6.1.3.4	○	○	○			ツール検証結果	10.2.6	②	②	②		
5	ツールソースコードは下位ツール要求にトレース可能である。	6.1.3.4.e	6.1.3.4	○	○	○			ツール検証結果	10.2.6	②	②	②		
6	ソースコードは正確であり、一貫している。	6.1.3.4.f	6.1.3.4	●	○	○			ツール検証結果	10.2.6	②	②	②		

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

【Table T-5】

ここではツールコーディングプロセスの成果物であるソースコードに対するレビュー／分析について説明する。レビューのポイントは表に挙げた6項目である。

《6.1.3.4》ツールソースコードのレビュ/分析(Reviews and Analyses of the Tool Source Code)

これらのレビュー/分析の目的は、ツールコーディングプロセスで入り込んだエラーを検出し、報告することである。これらのレビュー/分析はツールコーディングプロセスの成果物が正確で、完全で、検証可能であることを確認する。主な考慮事項には、下位ツール要求とツール構造に関するコードの正確性、ツールコード標準への準拠がある。これらのレビュー/分析はツールソースコードに限定され、外部コンポーネント検証についてはセクション6.1.4.3で述べられる。これらのレビュー/分析の活動はツールソースコードが以下の目的を満たすことを確認する。

a. 下位ツール要求への準拠:目的は、ツールソースコードが下位ツール要求に関して正確で完全であること、またソースコードがどんな記載されていないどんな機能も実現していないことを保証することである。

b. ツール構造への準拠: 目的はツールソースコードが、ツール構造で定義されたデータと矛盾がないことを保証することである。

c. 検証可能性: 目的は、ツールソースコードが検証できないステートメントと構造 (structures)を含まないことを保証することである。

d. 標準への準拠: 目的は、ツールコード標準がコード開発の間中ずっと適用され続け、また標準からの逸脱が正当化されることを保証することである。

e. トレーサビリティ: 目的は、下位ツール要求がツールソースコードへ落とし込まれたことを保証することである。

f. 正確性と一貫性: 目的は、ツールソースコードの正確さ及び一貫性(固定小数点数演算のオーバーフロー及び解決 (resolution), 浮動小数点数演算、リソース競合と制限、例外処理、初期化していない変数の使用、未使用の変数や定数、タスク競合によるデータ破壊を含む)を決定することである。

《6.1.3.4》

4.4.3 ツール資格データ

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

(1) ツールソースコード(Tool Source Code)

各コンポーネントに対して、ツールソースコードは以下から構成される。

(1)スクリプトやソース言語で書かれたコード
(2) リンク命令 (linking instructions)
(3) コンパイラ命令(compiler instructions)

このデータには、名前、リビジョンの日付、それと(もしくは)バージョンをなどのツール識別がなければならない。

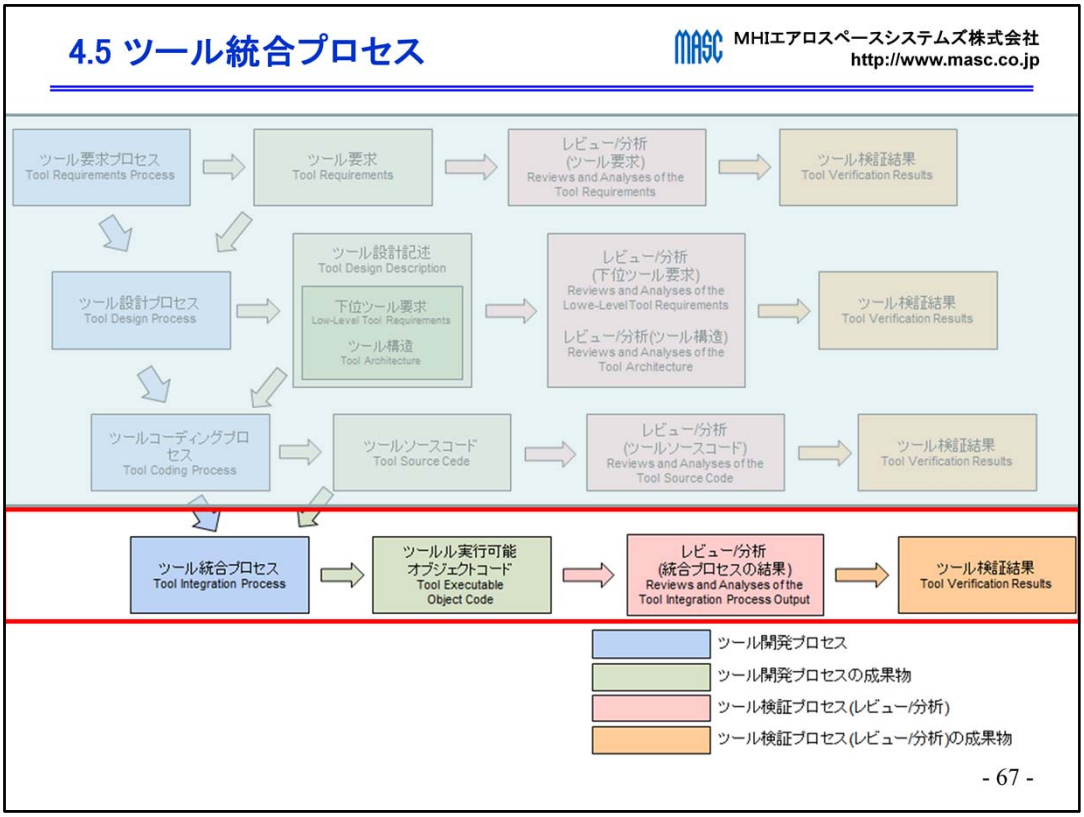
- 66 -

【10.2.3】

《10.2.3》ツールソースコード (Tool Source Code)

各ツールソースコードコンポーネントに関して、このデータは (1)スクリプトやソース言語で書かれたコード, (2) リンク命令(linking instructions), (3) ツールソースコードからツール実行可能オブジェクトソースコードを生成するためのコンパイラ命令(compiler instructions)(もし利用できるなら、言語に依存する)から成る。このデータには便宜、名前、リビジョンの日付、それと(もしくは)バージョンなどのツール識別がなければならない。

《10.2.3》



【5.2.4】

ここでは、ツール統合プロセス(Tool Integration Process)について説明する。

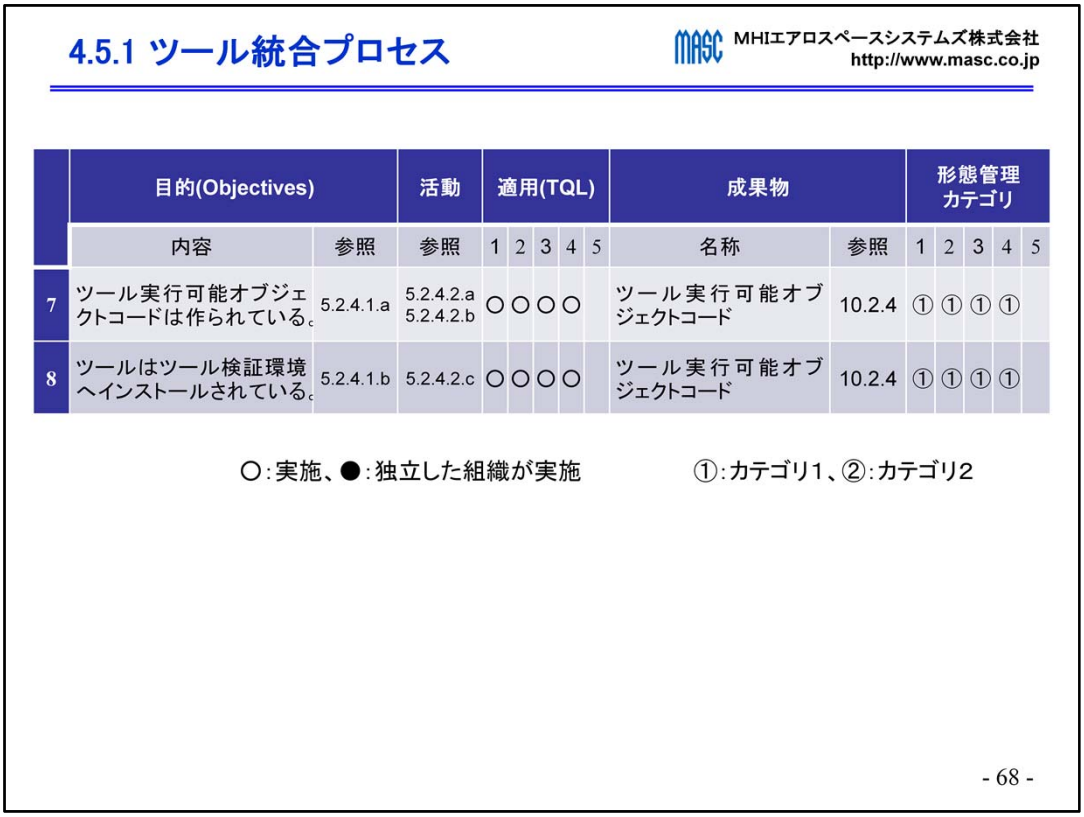
ツール統合プロセスは、ツールソースコードからツール実行可能オブジェクトコードを生成するプロセスである。これは、ツール開発環境でツールソースコードをコンパイル・リンクすることによって実現される。ツール開発環境とツール検証環境が異なる場合、ツール実行可能オブジェクトコードはツール検証環境にインストールされなければならない。

ツール資格計画プロセス(Tool Qualification Planning Process)より以下をインプットとして受ける。

(a) ツール開発計画(Tool Development Plan)

ツールコーディングプロセス(Tool Coding Process)より以下をインプットとして受ける。

(a) ツールソースコード(Tool Source Code)



4.5.1 ツール統合プロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
7	ツール実行可能オブジェクトコードは作られている。	5.2.4.1.a	5.2.4.2.a 5.2.4.2.b	○	○	○	○		ツール実行可能オブジェクトコード	10.2.4	①	①	①	①	
8	ツールはツール検証環境へインストールされている。	5.2.4.1.b	5.2.4.2.c	○	○	○	○		ツール実行可能オブジェクトコード	10.2.4	①	①	①	①	

○：実施、●：独立した組織が実施　　①：カテゴリ1、②：カテゴリ2

- 68 -

【Table T-2】

ツール統合プロセスは、ツールの実行形式でツールを作成することから構成される。

《5.2,4.1》ツール統合の目的(Tool Integration Objectives)

ツール統合プロセスの目的は：

a. ツール実行可能オブジェクトコードがツール開発環境で生成される。

b. ツール実行可能オブジェクトコードがツール検証環境へインストールされる。

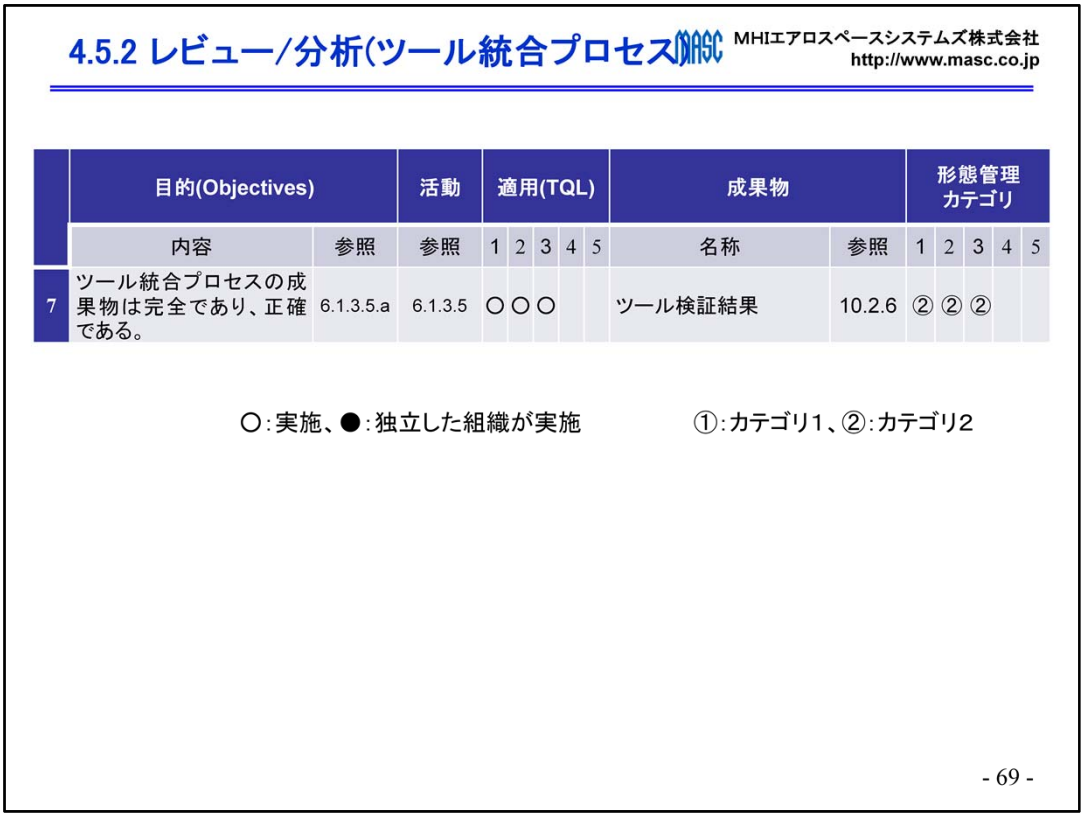
《5.2.4.1》ツール統合の活動(Tool Integration Activities)

このプロセスの活動は：

a. ツール実行可能オブジェクトコードが、ツールソースコード及びコンパイラとリンクの命令から生成されなければならない。ツール実行可能オブジェクトコードは、時々設定ファイルのような他のファイルを含むことに注意しなければならない。

b. ツール統合プロセスの間に検出された不十分な又は誤った入力は、不十分な又は誤った入力を生産したプロセスへ提供されなければならない。

c. もしツール検証環境がツール開発環境と異なる場合、又は複数のツール検証環境がある場合、ツール実行可能オブジェクトコードはツール検証環境にインストールされなければならない。



4.5.2 レビュー/分析(ツール統合プロセス)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
7	ツール統合プロセスの成果物は完全であり、正確である。	6.1.3.5.a	6.1.3.5	○	○	○			ツール検証結果	10.2.6	②	②	②		

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

- 69 -

【Table T-5】

ツール統合プロセスの成果物が完全であることを保証する。これは、コンパイル及びリンク結果の検証により実行することができる。ここでは、コンパイラの警告、コンポーネント不足、不正確なコンポーネントインターフェースなどを検証する。

《6.3.5》ツール統合プロセスの成果物のレビュー/分析(Reviews and Analyses of the Tool Integration Process Output)

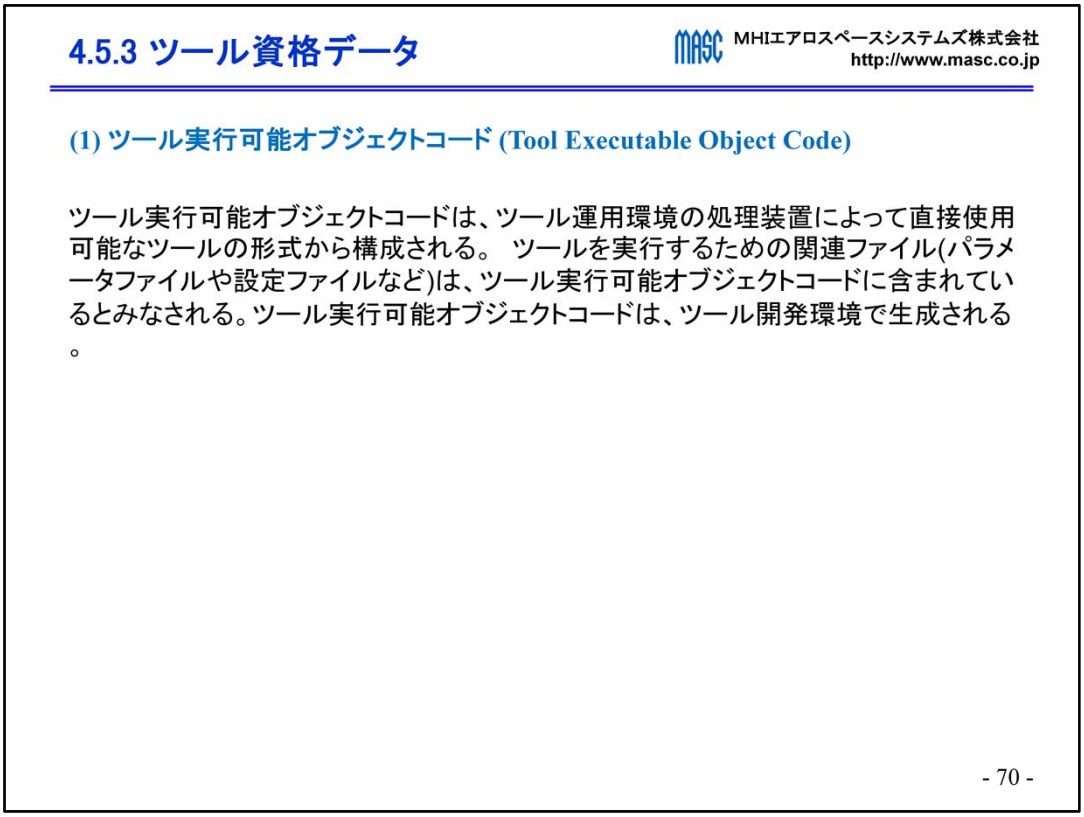
これらのレビュー/分析の目的は、ツール統合プロセスで入り込んだエラーを検出し、報告することである。
目的は:

a.　ツール統合プロセスの成果物が完全で正しいことを保証すること。

活動には、コンパイル/リンクデータの詳細な検査の実施がある。
潜在的エラーの典型例には以下のものがある。

・コンパイラの警告
・コンポーネント不足
・不正確なコンポーネントインターフェース

《6.3.5》



【10.2.3】

本プロセスの成果物はツール実行可能オブジェクトコード(Tool Executable Object Code)である。

《10.2.3》ツール実行可能オブジェクトコード(Tool Executable Object Code)

ツール実行可能オブジェクトコードは、ツール運用環境の処理装置(processing unit)によって直接使用可能なツールの形式から成る。それは、選択されたソースコード言語、コンパイル(compiling)、及びリンク(linking)への依存は必要ないかもしれないことに注意しなければならない。一つの例は、スクリプト言語で実現されたツールである。この場合、ツール実行可能オブジェクトコードは、その実行可能形式内でのツールだと理解されなければならない。

ツールを実行するため要求されるパラメータ及び設定ファイルのような関連ファイルは、ツール実行可能オブジェクトコードに含まれているとみなされる。ツール実行可能オブジェクトコードは、ツール開発環境で生成される。ツールがマルチツール運用環境で使われると意図される場合、複数のツール実行可能オブジェクトコードの設定(configurations)が生成されても良い。

《10.2.3》

4.6 トレーサビリティ

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

ツール開発プロセスにおけるトレーサビリティ

以下の双方向のトレーサビリティを示すトレースデータが作らなければならない。

(1) ツール運用要求　⇔　ツール要求

(2) ツール要求　⇔　下位ツール要求

(3) 下位ツール要求　⇔　ツールソースコード

- 71 -

【5.2.5】

《6.1.5》ツール開発プロセスにおけるトレーサビリティ (Tool Development Process Traceability)

ツール開発プロセスのトレーサビリティの活動は:

a. トレースデータ(ツール運用要求とツール要求の間で双方向の関係を見せている) が以下の目的のため開発される。

1. ツール運用要求の完全な実現の検証を可能とする。
2. ツール運用要求へ直接トレース可能ではないそれらの派生要求に可視性を与える。

b. トレースデータ(ツール要求と下位ツール要求の間で双方向の関係を見せている)が以下の目的のため開発される。

1. ツール要求の完全な実現の検証を可能とする。
2. ツール要求へ直接にトレース可能ではないそれらの派生下位要求へ、またツール設計プロセスの間に作成される構造設計決定への可視性を与える(?).

c. トレースデータ(下位ツール要求とツールソースコードの間の双方向の関係を見せている)が以下の目的で作成される。

1. ツールソースコードが記載のない機能を実現しないという検証を可能とする。
2. 下位ツール要求の完全な実現の検証を可能とする。

《6.1.5》

5. ツールテストプロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

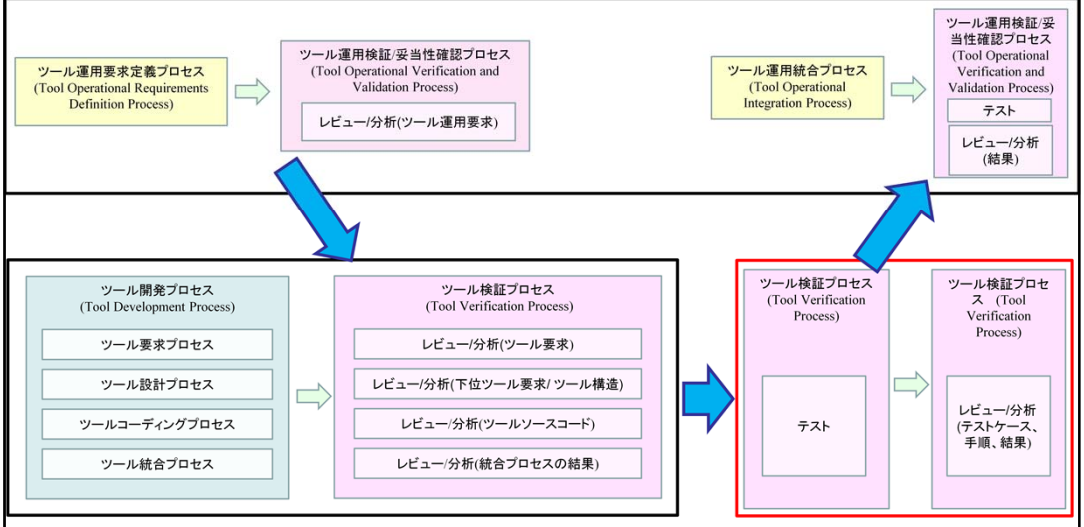
ツールテストプロセス
(Tool Test Process)

1. ツールテストプロセスのフロー
2. ツールテスト
3. テストの流れ
4. 要求ベーステスト
5. テストカバレッジ分析
6. ソフトウェアテストプロセスの目的
7. レビュー／分析
8. トレーサビリティ

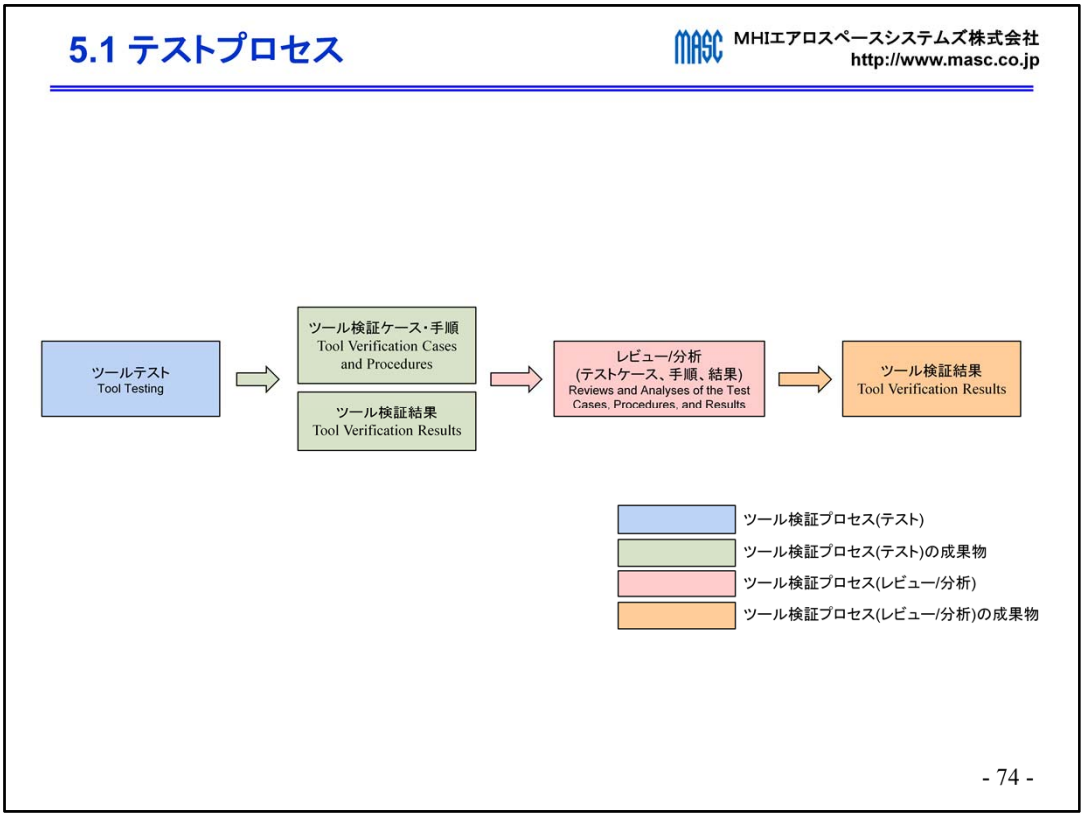
【6.1.4】

5. ツールテストプロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp



- 73 -



【6.1.4】

作成したツールの動作をテストするプロセスについて説明する。

先にも述べたようにDO-330では、明確にテストをプロセスとして規定しておらず、ツール検証プロセス(Tool Verification Process)内にテストを定義している。

ここで、DO-178ではテスト対象により3つのテストを定義していた。

(1) ハードウェア／ソフトウェア統合テスト(Hardware/software Integration Testing)
ソフトウェア上位要求、ソフトウェア構造のテスト

(2) ソフトウェア統合テスト(Software Integration Testing)
ソフトウェア上位要求、ソフトウェア構造のテスト

(3) ソフトウェア下位要求テスト(Low-level Testing)
ソフトウェア下位要求

一方で、DO-330では1つのテストのみ定義されており、
そのテストを通して規約を満足するようなテスト計画を立てることになる。

5.2 ツールテスト

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

ツールテストの目的は以下の2点である。

(1) ツールがその要求を満足していることを確認する
(2) 受け入れ難い故障状態に陥るようなエラーが取り除かれていることを確認する。

また、その目的を達成するために、テストケースは要求(ツール要求、下位ツール要求)をベースとすること。

- 75 -

【6.1.4】

《6.1.4》 ツールテスト (Tool Testing)

ツールテストプロセスは、ツールがその要求を満たすこと、またツール機能に影響を与えるエラーが除去されたことを高い信頼度で確認するために利用される。

《6.1.4》

《6.1.4.1》 ツールテストの目的(Tool Testing Activities)

ツールテストの目的は、下記事項を確認するため、ツール実行可能オブジェクトコードを実行することである。

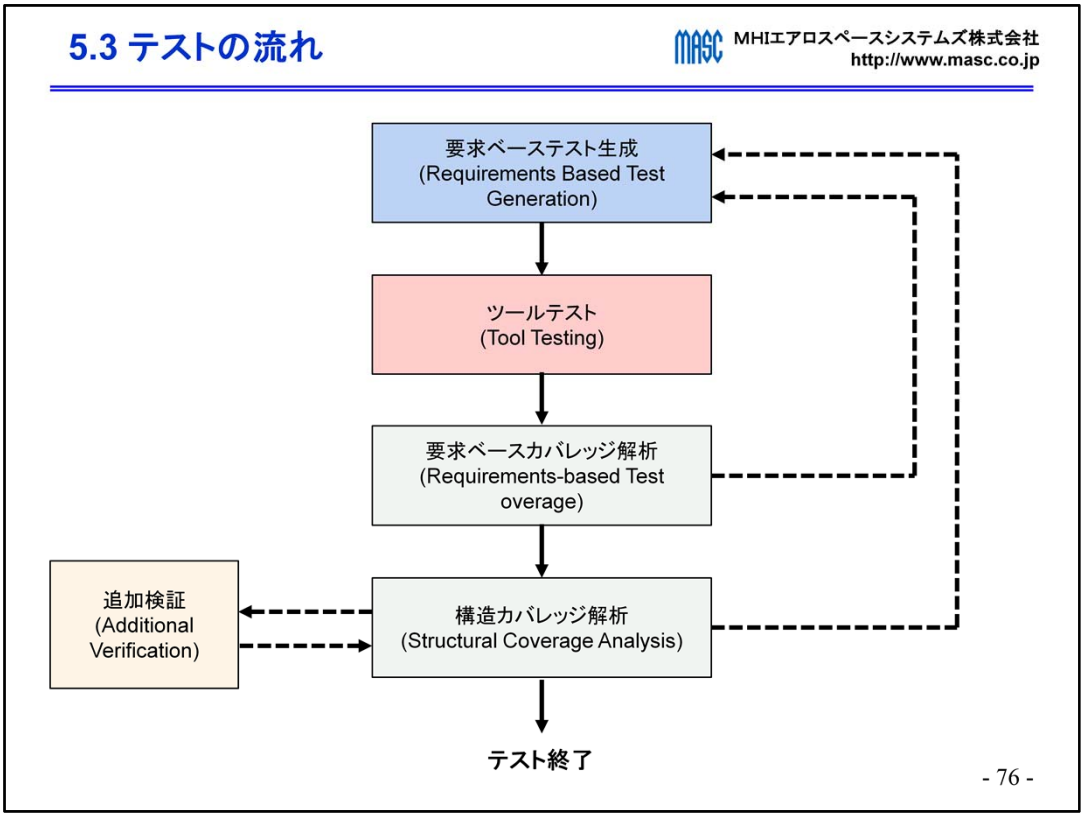
a. ツール実行可能オブジェクトコードがツール要求に従う。

b. ツール実行可能オブジェクトコードがツール要求にロバストである。

c. ツール実行可能オブジェクトコードが下位ツール要求に従う。

d. ツール実行可能オブジェクトコードが下位ツール要求にロバストである。

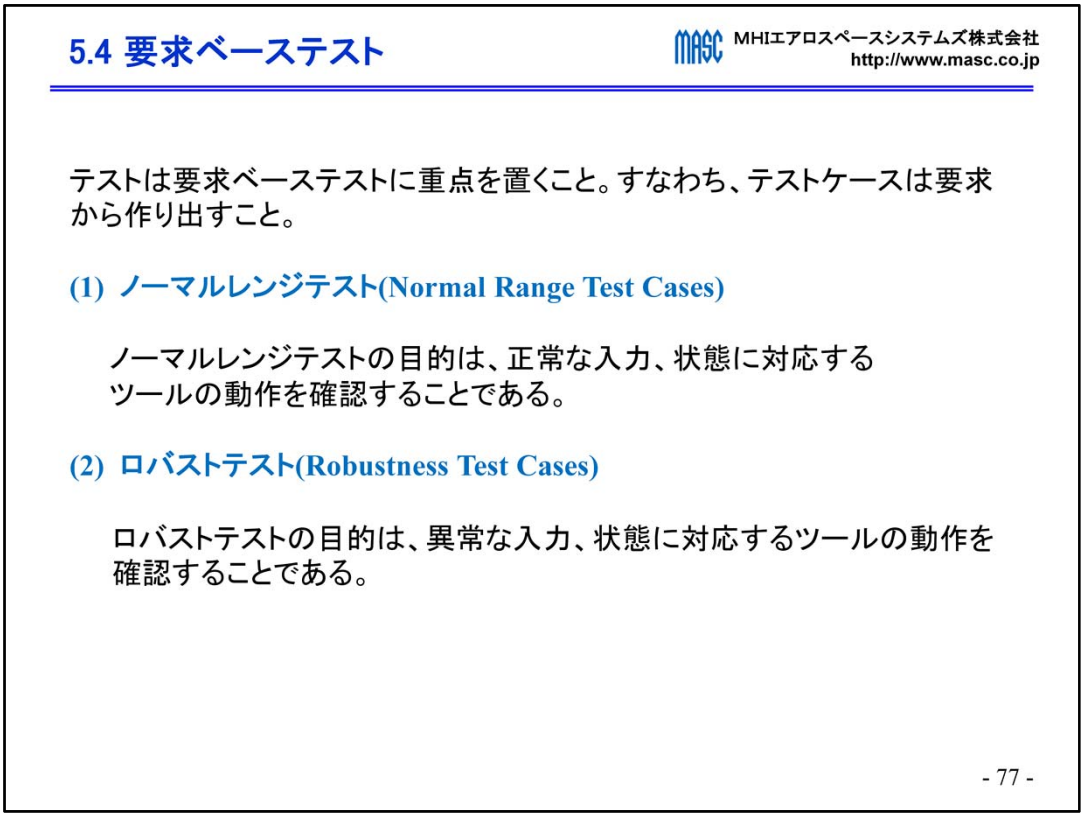
《6.1.4.1》



【6.1.4.2】

このフローでは、テストプロセスの活動を示している。

先に記述したように、ツールテストの結果としてツール要求カバレッジ解析、ツール構造カバレッジ解析を求めている。



【6.1.4.2】

テストは要求ベーステストに重点を置くこととしている。これは、開発の各段階において上下の関係のトレーサビリティが取れているため、要求ベーステストであってもコードのカバレッジは確保できるということであろう。

テストケースとしては、ノーマルレンジテストとロバストテスト（異常範囲テスト）の2つのテストの実施すること。

(1) ノーマルレンジテスト(Normal Range Test Cases)

ノーマルレンジテストの目的は、正常な入力、状態に対応するソフトウェアを確認することである。

(a) 実数及び整数入力データは、妥当な同値クラスと境界値を使って実行されなければならない。

(b) 状態遷移では、正常オペレーションにおける可能な遷移を全て実行すること。

(c) 論理式で表現された要求では、全てのブール演算の組み合わせを検証すること。

(2) ロバストテスト(Robustness Test Cases)

ロバストテストはツール要求で識別された全ての故障モード(例えば、異常起動モード、矛盾した入力など)に対処するため実行されなければならい。

《6.1.4.2》ツールテストの活動(Tool Testing Activities)

要求ベーステストが強調されるのは、エラーを発見することにおいて、この戦略が最も有効であると発見されたからである。要求ベーステストケースの選択の活動には以下の事項がある。

a. テストケース/手順は、ツールがその要求を満たすことを確認するために開発されなければならない。

・各テストケースは要求(ツール要求又は下位ツール要求)から作成され、入力セット、条件、期待される結果、合否判定基準を明らかにする。

・テスト手順はテストケースから生成される。

・トレースデータはテストケースとテスト手順の間で生成される。

b. ノーマルレンジテストは、以下の事項を含み、実行されなければならない。

・実数及び整数入力データは、妥当な同値クラスと境界値を使って実行されなければならない。

・状態遷移に関して、テストケースは正常オペレーションの間に起こりうる遷移を実行するため作成されなければならない。

・論理式表現される要求のため、又は入力論理の組み合わせを含む要求のため、ノーマルテストケースは変数使用とブール演算を検証しなければならない。特に、TQL-1に関して、テストケースは固定した全ての他の可能な要求条件を保持している間に、その要求条件を変更することによって各要求条件が独立して要求された結果に影響をおよぼすことを示さなければならない。

c. ロバストテストはツール要求で識別された全ての故障モード(例えば、異常起動モード、矛盾した入力など)に対処するため実行されなければならい。

d. もし必要なら、以下の事項の確認を完全なものにするため、追加のロバストテストも作成されなければならない。

・異常な入力や条件に応答するツール能力

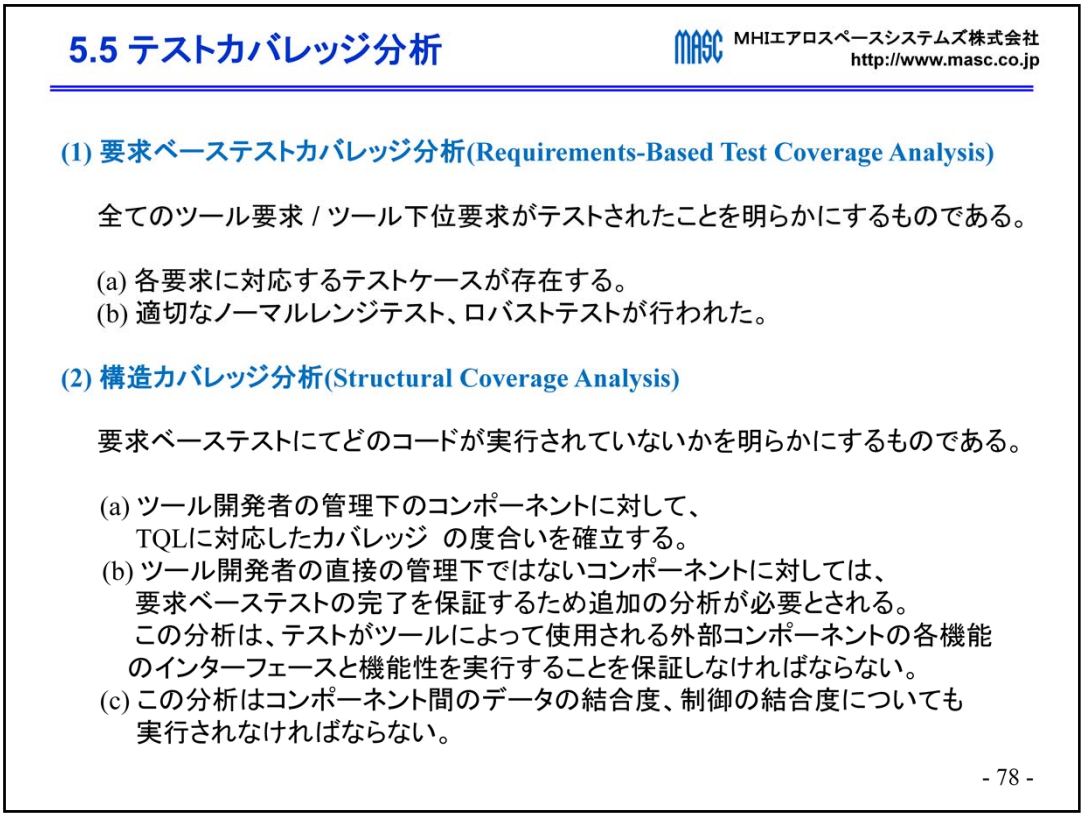
・異常な振る舞いの検出

・無効な出力の防止

注意事項: ロバストテストケースは要求ベースである。ツール要求が異常な条件や入力への正しい応答を詳細に明記しない場合、ロバストテスト基準を十分に満たせない。テストケースはツール要求の不備を明らかにし、そのケースではツール要求は修正される。逆に、要求の十分なセットが存在する場合、ロバストテストケースはそれらのツール要求に従うだろう(*exists that~ の文法不明)

要求ベーステストカバレッジ分析は全ての要求(ツール要求及び下位ツール要求)がテストされたことを確認するため行わなければならい。この分析は各要求が少なくとも一つのテストケースを持っていること、及び適切なノーマル/ロバストテストが行われたことを保証する。

《6.1.4.2》



5.5 テストカバレッジ分析

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

(1) 要求ベーステストカバレッジ分析(Requirements-Based Test Coverage Analysis)

全てのツール要求 / ツール下位要求がテストされたことを明らかにするものである。

(a) 各要求に対応するテストケースが存在する。
(b) 適切なノーマルレンジテスト、ロバストテストが行われた。

(2) 構造カバレッジ分析(Structural Coverage Analysis)

要求ベーステストにてどのコードが実行されていないかを明らかにするものである。

(a) ツール開発者の管理下のコンポーネントに対して、
TQLに対応したカバレッジ の度合いを確立する。
(b) ツール開発者の直接の管理下ではないコンポーネントに対しては、
要求ベーステストの完了を保証するため追加の分析が必要とされる。
この分析は、テストがツールによって使用される外部コンポーネントの各機能
のインターフェースと機能性を実行することを保証しなければならない。
(c) この分析はコンポーネント間のデータの結合度、制御の結合度についても
実行されなければならない。

- 78 -

【6.4.4】

テストカバレッジ分析には、以下の2種類がある。

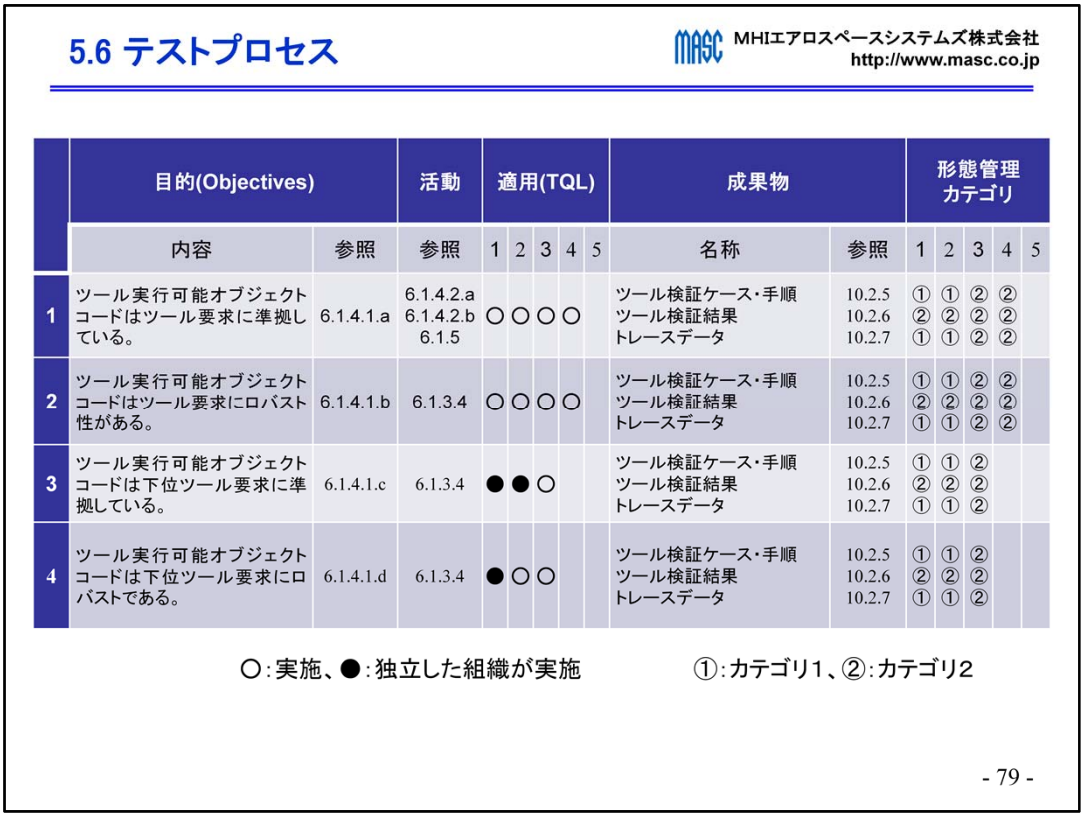
(1) 要求ベーステストカバレッジ分析(Requirements-Based Test Coverage Analysis)

ソフトウェア要求の実装がどのくらい検証されているかを明らかにするものである。この分析は追加の要求ベーステストケースの必要性を明らかにする。

(a) 各ソフトウェア要求に対応するテストケースが存在する。
(b) テストケースがノーマル、ロバストネステストの評価基準を満足していること。

(2) 構造カバレッジ分析(Structural Coverage Analysis)

要求ベーステストにてどのコードが実行されていないかを明らかにするものである。要求ベーステスト実行後、全てのコードが実行されていない場合、追加の検証が必要となる。



5.6 テストプロセス

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
1	ツール実行可能オブジェクトコードはツール要求に準拠している。	6.1.4.1.a	6.1.4.2.a 6.1.4.2.b 6.1.5	○	○	○	○		ツール検証ケース・手順 ツール検証結果 トレースデータ	10.2.5 10.2.6 10.2.7	① ② ①	① ② ①	② ② ②	② ② ②	
2	ツール実行可能オブジェクトコードはツール要求にロバスト性がある。	6.1.4.1.b	6.1.3.4	○	○	○	○		ツール検証ケース・手順 ツール検証結果 トレースデータ	10.2.5 10.2.6 10.2.7	① ② ①	① ② ①	② ② ②	② ② ②	
3	ツール実行可能オブジェクトコードは下位ツール要求に準拠している。	6.1.4.1.c	6.1.3.4	●	●	○			ツール検証ケース・手順 ツール検証結果 トレースデータ	10.2.5 10.2.6 10.2.7	① ② ①	① ② ①	② ② ②		
4	ツール実行可能オブジェクトコードは下位ツール要求にロバストである。	6.1.4.1.d	6.1.3.4	●	○	○			ツール検証ケース・手順 ツール検証結果 トレースデータ	10.2.5 10.2.6 10.2.7	① ② ①	① ② ①	② ② ②		

○：実施、●：独立した組織が実施　　①：カテゴリ1、②：カテゴリ2

- 79 -

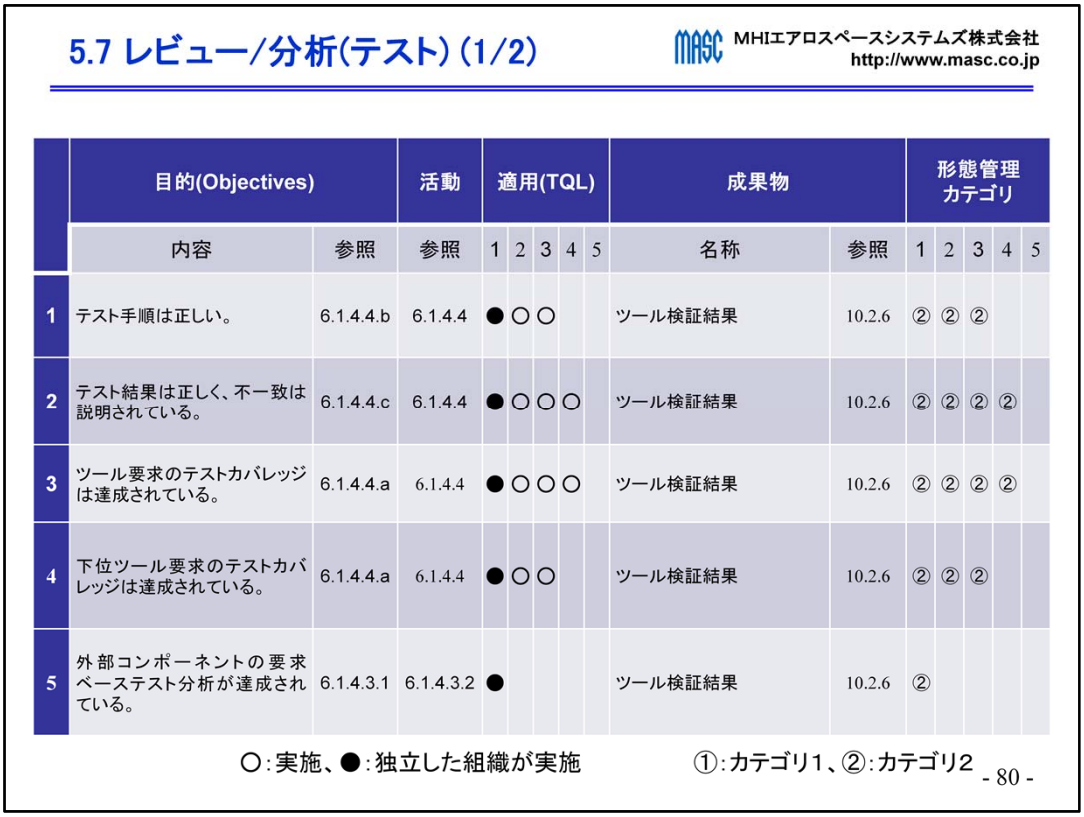
【Table T-6】

この表はテストプロセスの実行に関しての規定を定めている。

1項、2項は、ツール要求に対するノーマルレンジテスト、ロバストテストを対象とている。

3項、4項は、下位ツール要求に対するノーマルレンジテスト、ロバストテストを対象としている。

下位ツール要求テストの一部は独立した第3者の実施を求めている。また、TQLが4の場合は、その実施を要求していない。



5.7 レビュー/分析(テスト)(1/2)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
1	テスト手順は正しい。	6.1.4.4.b	6.1.4.4	●	○	○			ツール検証結果	10.2.6	②	②	②		
2	テスト結果は正しく、不一致は説明されている。	6.1.4.4.c	6.1.4.4	●	○	○	○		ツール検証結果	10.2.6	②	②	②	②	
3	ツール要求のテストカバレッジは達成されている。	6.1.4.4.a	6.1.4.4	●	○	○	○		ツール検証結果	10.2.6	②	②	②	②	
4	下位ツール要求のテストカバレッジは達成されている。	6.1.4.4.a	6.1.4.4	●	○	○			ツール検証結果	10.2.6	②	②	②		
5	外部コンポーネントの要求ベーステスト分析が達成されている。	6.1.4.3.1	6.1.4.3.2	●					ツール検証結果	10.2.6	②				

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

- 80 -

【Table T-7】

この表はテストプロセスにおけるレビュー／分析に関しての規定を定めており、コードのテストが正確に、完全に実行されていることを保証するものである。

1項は、テストケースが正確にテスト手順と期待値に反映されていることを求めている。
2項は、テスト結果が正しく、期待値と実行値に差があった場合はその説明がされていることを求めている。
3項、4項は要求カバレッジの達成を要求するものである。
TQL-4は、前の表で下位ツール要求テストを要求していないので、ここでも適用外となっている。

TQL-1に関しては、このレビュー／分析は全て独立した第3者が実施することを求めている。

《6.1.4.4》テストケース、手順、結果のレビュー/分析(Reviews and Analyses of the Test Cases, Procedures, and Results)

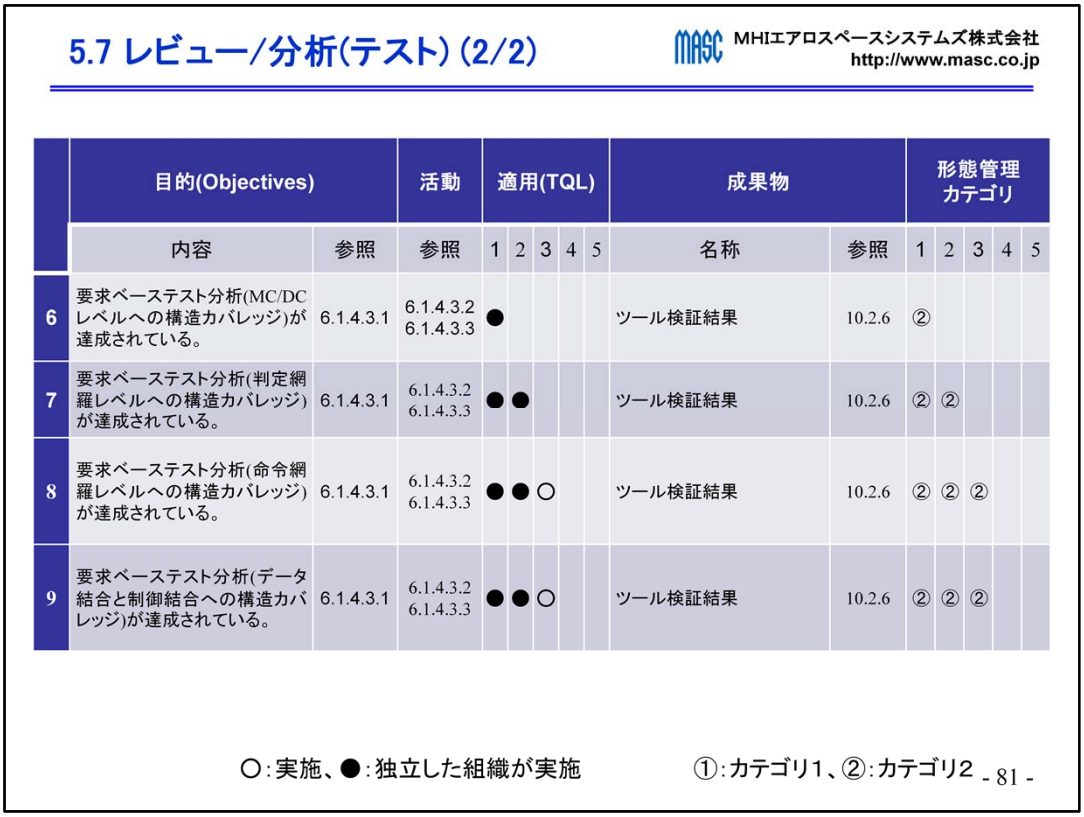
これらのレビュー/分析の目的は、コードのテストが正確かつ完全に作成され実行されたかを保証することである。これらのレビュー/分析の活動はツールテストが以下の目的を満たすことを確認する。

a. テストケース: 目的は、全ての要求のテストカバレッジが達成されることを保証することである(関連する活動については6.1.4.2.eを参照)。

b. テスト手続き: 目的は、テストケース(期待する結果を含む)がテスト手続きに正しく落とし込まれたことを検証することである。

c. テスト結果: 目的は、テスト結果が正しいこと、及び実際の結果と期待した結果の間の矛盾が説明されることを保証することである。

《6.1.4.4》



5.7 レビュー/分析(テスト) (2/2)

MASC MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
6	要求ベーステスト分析(MC/DCレベルへの構造カバレッジ)が達成されている。	6.1.4.3.1	6.1.4.3.2 6.1.4.3.3	●					ツール検証結果	10.2.6	②				
7	要求ベーステスト分析(判定網羅レベルへの構造カバレッジ)が達成されている。	6.1.4.3.1	6.1.4.3.2 6.1.4.3.3	●	●				ツール検証結果	10.2.6	②	②			
8	要求ベーステスト分析(命令網羅レベルへの構造カバレッジ)が達成されている。	6.1.4.3.1	6.1.4.3.2 6.1.4.3.3	●	●	○			ツール検証結果	10.2.6	②	②	②		
9	要求ベーステスト分析(データ結合と制御結合への構造カバレッジ)が達成されている。	6.1.4.3.1	6.1.4.3.2 6.1.4.3.3	●	●	○			ツール検証結果	10.2.6	②	②	②		

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

【Table T-7】

この表では、構造カバレッジ分析について定めている。

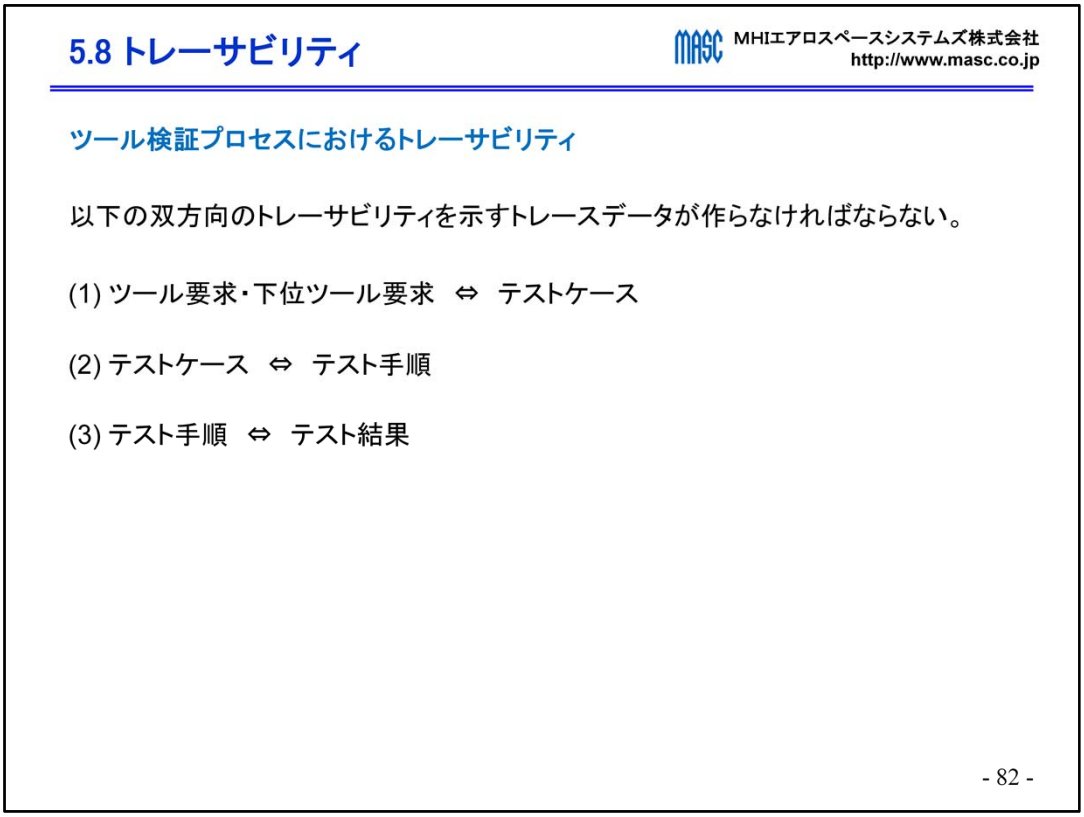
TQL-4では、構造カバレッジ分析は求められていない。すなわちツール要求の要求カバレッジのみが求められている。

8項はいわゆるC0カバレッジのことであり、TQL-3以上で要求されている。

7項はいわゆるC1カバレッジのことであり、TQL-2以上で要求されている。

TQL-1では、それに加えてMCDCのカバレッジを要求されている。

ちなみに、全体としてTQL-1とTQL-2との適用項目の違いはこの5項(前ページ)と6項のみである。



【6.1.5】

《6.1.5》ツール検証プロセスのトレーサビリティ(tool Verification Process Traceability)

ツール検証プロセスのトレーサビリティの活動は:

a. トレースデータが、下位ツール要求とその関連するテストケースだけでなく、ツール要求とそれらに関連するテストケースの間の双方向関連を見えるようにするため作成される。このトレースデータの目的は、要求ベーステストカバレッジ分析を支援することである。

b. トレースデータが、テストケースとテスト手続き間の双方向関係を見えるようにするため作成される。トレースデータの目的は、テストケースの完全なセットがテスト手続きへ落とし込まれたという検証を可能とすることである。

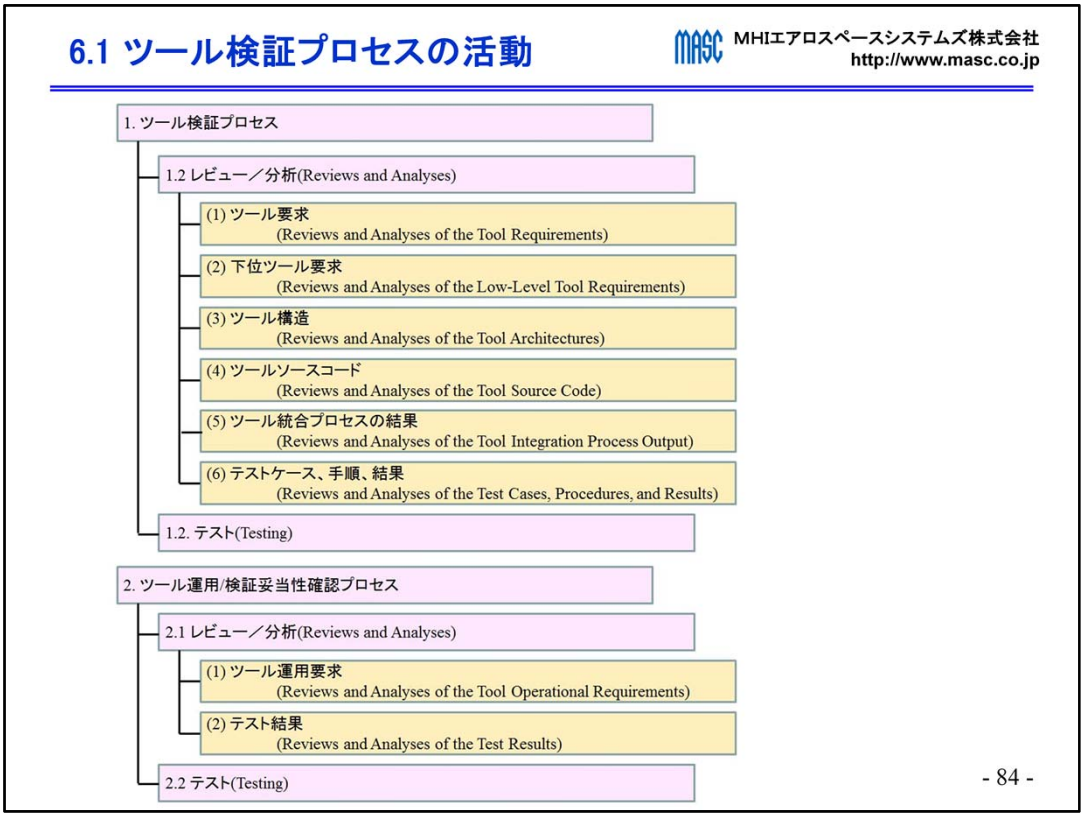
c. トレースデータが、テスト手続きとテスト結果の間の双方向関係を見えるようにするため作成される。トレースデータの目的は、テスト手続きの完全なセットが実行されたという検証を可能とすることである。

《6.1.5》

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

ツール検証プロセス
(Tool Verification Process)

1. ツール検証プロセスの活動
2. 成果物


6.1 ツール検証プロセスの活動
MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp
1. ツール検証プロセス
1.2 レビュー／分析(Reviews and Analyses)
(1) ツール要求
(Reviews and Analyses of the Tool Requirements)
(2) 下位ツール要求
(Reviews and Analyses of the Low-Level Tool Requirements)
(3) ツール構造
(Reviews and Analyses of the Tool Architectures)
(4) ツールソースコード
(Reviews and Analyses of the Tool Source Code)
(5) ツール統合プロセスの結果
(Reviews and Analyses of the Tool Integration Process Output)
(6) テストケース、手順、結果
(Reviews and Analyses of the Test Cases, Procedures, and Results)
1.2. テスト(Testing)
2. ツール運用/検証妥当性確認プロセス
2.1 レビュー／分析(Reviews and Analyses)
(1) ツール運用要求
(Reviews and Analyses of the Tool Operational Requirements)
(2) テスト結果
(Reviews and Analyses of the Test Results)
2.2 テスト(Testing)
- 84 -

【6】

ツール検証プロセスは、
ツール検証プロセスおよびツール運用/検証妥当性確認プロセスから構成される。
前述した通り、ツール検証プロセスは、プロセスはツール開発プロセスと並行して実施される。
既に先に説明したのでその参照先を以下に記述する。

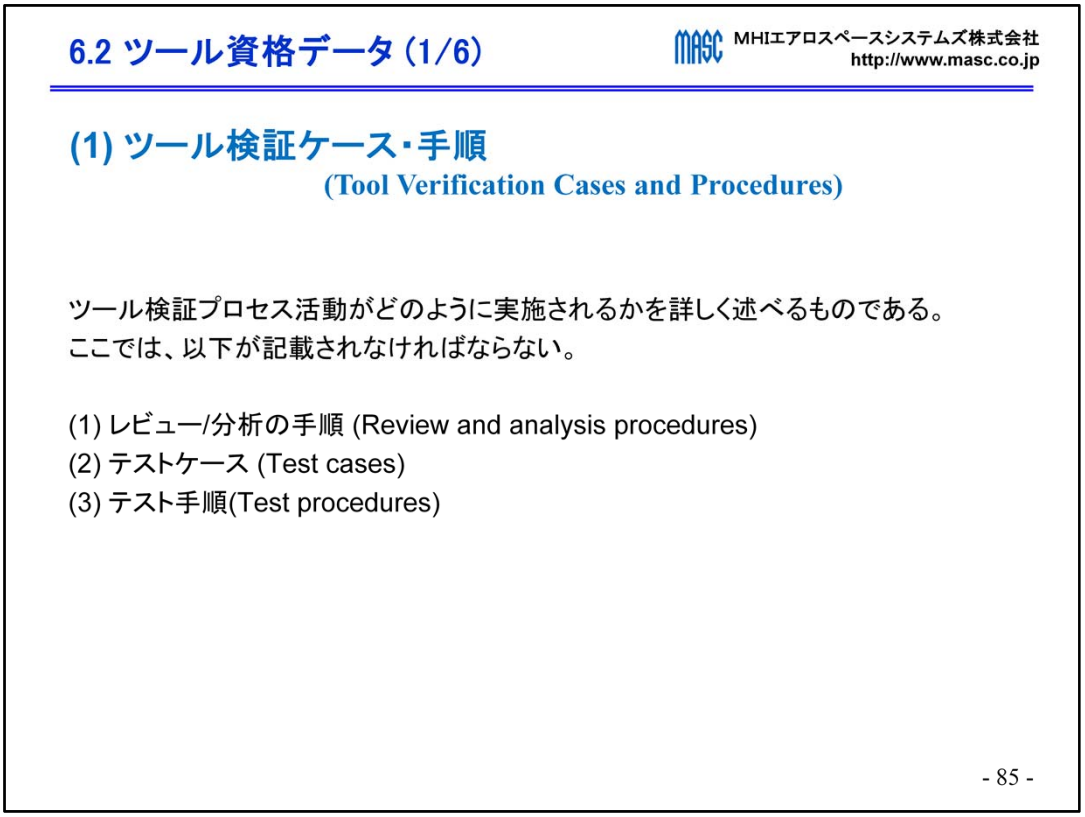
1. ツール検証プロセス
1. 2. レビュー／分析(Reviews and Analyses)

(1) ツール要求(Reviews and Analyses of the Tool Requirements)
3.3.1.2 レビュー／分析（ツール要求）参照。
(2) 下位ツール要求(Reviews and Analyses of the Low-Level Tool Requirements)
3.3.2.2 レビュー／分析（下位ツール要求）参照。
(3) ツール構造(Reviews and Analyses of the Tool Architectures)
3.3.2.2 レビュー／分析（ソフトウェア構造）参照。
(4) ツールソースコード(Reviews and Analyses of the Tool Source Code)
3.3.3.2 レビュー／分析（ソースコード）参照。
(5) ツール統合プロセスの結果(Reviews and Analyses of the Tool Integration Process Output)
3.3.4.2 レビュー／分析（ツール統合プロセスの結果）参照。
(6) テストケース、手順、結果Reviews and Analyses of the Test Cases, Procedures, and Results)
4.7 レビュー／分析（テスト）参照。

2. ツール運用/検証妥当性確認プロセス
2.1 レビュー/分析
(1) ツール運用要求
3.2.3 レビュー/分析(ツール運用)を参照。

(2) テスト結果

3.3.3 ツール運用統合プロセス(テスト)を参照。



【10.2.5】

(1)レビューと分析手順は、レビュー／分析に先立ってその詳細計画を作成するものである。
(2)テストケース(3)テスト手順は、テストプロセスの手順を作成するものである。

《10.2.5》ツール検証ケース・手順 (Tool Verification Cases and Procedures)

ツール検証ケース/手順は、どのようにツール検証プロセス活動が実現されるかを詳細に記載する。このデータには以下の項目が含まれる。

a. レビュー/分析の手順: ツール検証計画での記載に加え、使用されるレビューや分析方法の範囲と深さ

b. テストケース: 各テストケースの目的、入力セット、条件、要求されるカバレッジ基準を達成するための期待される結果、そして合格/不合格基準

c. テスト手順:どのように各テストケースがセットアップされ実行されるかに関する順を追っての指示、どのようにテスト結果が評価されるか、そして使用されるテスト環境

《10.2.5》

6.2 ツール資格データ (2/6)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

(2) ツール検証結果(Tool Verification Results)

ツール検証プロセス(Tool Verification Process)の結果を記載する。

ここでは、以下が記載されなければならない。

(1) 各レビュー、分析、テストにおける、活動の間の良否の過程と、最終的な良否の結果を示す。
(2) レビュー、分析、テストがなされた形態項目、またはソフトウェアバージョンを特定する。
(3) カバレッジ分析、トレーサビリティ分析を含んだテスト、レビュー、分析の結果を含む。
(4) 不適合報告プロセスを使用して発見された矛盾を報告し追跡する。

- 86 -

【10.2.6】

これは、前述のツール検証ケース・手順を受けて、実際に「レビュー／分析」「テスト」を実施した結果についてまとめるものである。

《10.2.6》 ツール検証結果(Tool Verification Results)

ツール検証結果はツール検証プロセス活動で作成され、以下の事項が行わなければならない。

a. 各レビュー/分析そしてテストのため、活動中に合格/不合格した各手順を示し、最終的な合格/不合格結果を示す。

b. レビュー/分析され、テストされた形態項目やソフトウェアバージョンを識別する。

c. カバレッジ分析及びトレーサビリティ解析などの、テスト、レビュー/分析の結果を含む。

d. 不適合報告プロセスを使用して発見された矛盾を報告し追跡する。

注意事項: このデータはツール運用検証/妥当性確認プロセス(これらは本資料のセクション10.3.3及び10.3.4で述べられる)で生産されたデータを含まない。

《10.2.6》

6.2 ツール資格データ (3/6)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

(3) ツールインストール報告 (Tool Installation Report)

ツール実行可能オブジェクトコードはツール運用環境へインストールされる。
このインストールの報告には、以下が記載されなければならない。

(1) ツール運用環境(ハードウェア、OS設定、インストールオプションなど)の識別
(2)設定ファイル、パラメータファイルを含むツール実行可能オブジェクトコードのバージョン識別
(3)必要なら、外部コンポーネントの識別
(4)ツールを実行する手段(コマンドライン、スクリプトファイルなど)の識別

- 87 -

【10.3.2】

《10.3.2》ツールインストール報告(Tool Installation Report)

ツール実行可能オブジェクトコードは、ツール運用環境へインストールされる。このインストールの報告は以下の項目を含むべきである。

a. ツール運用環境(ハードウェア、オペレーティングシステム設定、インストールされたオプションなど)の識別

b. 全ての設定ファイルやパラメータファイルなど、ツール実行可能オブジェクトコードのバージョンの識別

c. 必要なら、外部コンポーネントの識別

d. ツールを実行する手段(コマンドライン、スクリプトファイルなど)の識別。これは、ユーザーマニュアルへの参照を含めることができる。

注意事項: この情報はSECIに含まれても良い。

《10.3.2》

6.2 ツール資格データ (4/6)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

(4) ツール運用検証/妥当性確認ケースと手順
(Tool Operational Verification and Validation Cases and Procedures)

ツール運用検証/妥当性確認プロセスがどのように行われるかを詳細に記載するものである。

以下が記載されなければならない。

(1) レビュー/分析の手順
(2) テストケース
(3) テスト手順

- 88 -

【10.2.5】

(1)レビューと分析の手順は、レビュー／分析に先立ってその詳細計画を作成するものである。
(2)テストケース(3)テスト手順は、テストの手順を作成するものである。

《10.3.4》ツール運用検証/妥当性確認ケースと手順(Tool Operational Verification and Validation Cases and Procedures)

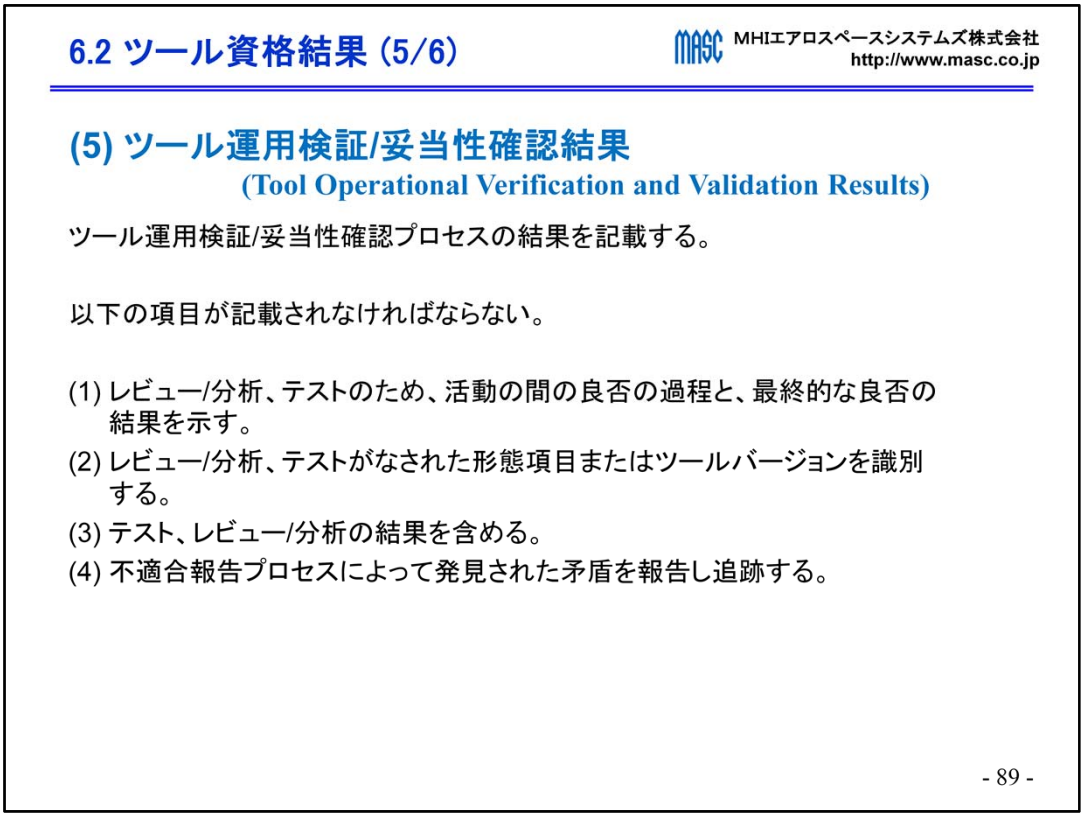
ツール運用検証/妥当性確認ケースと手順には、どのようにツール運用検証/妥当性確認プロセスの活動が行われるかを詳細に記述する。このデータは以下の項目を含まなければならない。

a. レビュー/分析の手順: ツール検証計画での記載に加え、使用されるレビュー/分析手法の範囲と深さ

b. テストケース: 合格/不合格の基準を達成するための各テストケースの目的、入力のセット、条件、そして期待される結果

c. テスト手順: どのように各テストケースがセットアップされ実行されるかについての順を追っての指示、どのようにテスト結果が評価されるか、そして使用されるテスト環境

《10.3.4》



【10.3.4】

これは、前述のツール運用検証/妥当性確認ケースと手順を受けて、実際に「テスト」「レビュー／分析」を実施した結果についてまとめるものである。

《10.3.4》ツール運用検証/妥当性確認結果(Tool Operational Verification and Validation Results)

ツール運用検証/妥当性確認プロセスではツール運用検証/妥当性確認結果を作成し、それは以下の項目をしなければならない。

各レビュー/分析、そしてテストのため、活動中に合格/不合格した手順を示し、最終的な合格/不合格結果を示す。

レビュー/分析され、テストされた形態項目やツールバージョンを識別する。

テスト、レビュー/分析の結果を含める。

不適合報告プロセスによって発見された矛盾を報告し追跡する。

《10.3.4》

6.2 ツール資格データ (6/6)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

(6) トレースデータ(Trace Data)

トレースデータは以下の双方向の関連性を立証するものである。

(1) ツール運用要求とツール要求
(2) ツール要求と下位ツール要求
(3) 下位ツール要求とツールソースコード
(4) ツール要求と
(5) テストケースとテストケース手順
(6) テスト手順とテスト結果

- 90 -

【10.2.7】

《10.2.7》トレースデータ(Trace Data)

トレースデータは、ライフサイクルデータ項目のコンテンツ間の関係を確立する。下記項目間の双方向関係を確認するトレースデータが作成されなければならない。

ツール運用要求とツール要求

ツール要求と下位ツール要求

下位ツール要求とツールソースコード

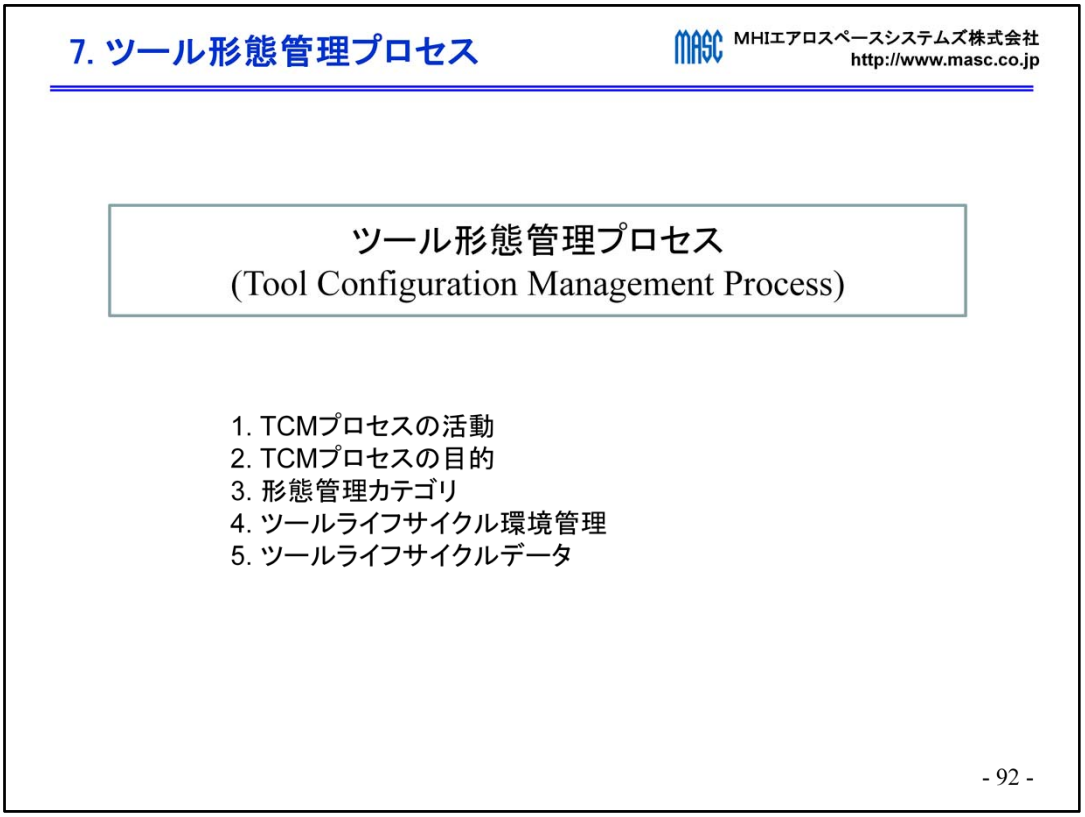
ツール要求と下位ツール要求、並びにそれらの関連テストケース

テストケースとテスト手続き

テスト手続きとテスト結果

注意事項: テスト手続きとテスト結果間のトレースデータはツール検証結果(10.2.6.cを参照)の一部であっても良い。

《10.3.4》



【7】

《7.0》ツール形態管理プロセス(Tool Configuration Management Process)

この章はツール形態管理(TCM)プロセスの目的と活動を説明する。TCMプロセスはツール計画プロセス(4参照)とツール形態管理計画(10.1.5参照)の定義が適用される。

TCMプロセスの成果物はツール形態管理記録(10.1.13参照)又は他のツールライフサイクルデータ内に記録される。

他のツールライフサイクルプロセスと協調して作用するTCMプロセスは下記を支援する。

(a) ツールライフサイクルを通して定義され管理されたツールの形態を提供する。

(b) 調査や改修のための要求がある場合、矛盾なくツール実行可能オブジェクトコードを複製する又はそれを再生成する能力を提供する。

(c) プロセス活動の一貫性と繰返し性を確かにする、ツールライフサイクル間のプロセス入力と成果物の管理を提供する。

(d) 形態項目とベースライン確立の管理によるレビューやステータス評価、変更管理のための既知点を提供する。

(e) 問題が注意を引き、変更が記録され、承認され、実装されることを確かにするための管理を提供する。

(f) ツールライフサイクルプロセスの成果物の管理によるツールの承認の証拠を提供する。

(g) 要求と適合するツール製品を評価する。

(h) 形態項目のために安全な物理的保管、回復、管理が維持されていることを確かにする。

《7.0》

【7.2】

1. 形態識別(Configuration Identification)

形態識別の目的は、各形態項目（とそのバージョン）を明白にラベル付けし、特定できるようにするものである。
形態識別は、ツールライフサイクルデータに付与される。ツールライフサイクルデータには、ツール製品そのものだけでなく各プロセスで作成された文書も含まれているため、当然のことながら、これらの文書も形態管理の対象となる。
ツール製品に対して形態識別を付ける際は、ツール製品を構成するコンポーネントにまでブレークダウンして付けることを定めている。原文では、”each separately controlled component”という表現がされている。
以降に出てくる変更管理やトレーサビリティにおいて対象を識別するためにも形態識別は用いられる。

2. ベースラインとトレーサビリティ(Baselines and Traceability)

ベースラインは、それ以降のツールライフサイクルプロセスにおいて使用する基本を決めるものである、と書かれており、文書であればA改訂、B改訂、ツール製品であればバージョンのことと解釈できる。
トレース可能という意味には2種類あり、変更等によりベースラインが変わるときには以前のベースラインとの間でトレース可能でなければならない、ということと、形態項目のベースラインがどの形態項目のベースラインをインプットとして作られたものなのかがトレース可能でなければならない。

3. 不適合の報告、追跡、是正処置(Software Configuration Management Process Activities)

ここで言う不適合には3種類ある。①ツールライフサイクルプロセスにおいて、ツール計画、標準に準拠していない、②ツールライフサイクルプロセスのアウトプットに欠陥がある、③ツール製品の異常なふるまいの3種類である。この不適合の報告、追跡、是正処置では、これらの不適合が記録され、解決されることを保証することを求めている。

《7.2》ツール形態管理プロセスの活動 (Tool Configuration Management Process Activities)

TCMプロセスとしては形態識別、変更管理、ベースライン確立、そして関連するツールライフサイクルデータを含むツール製品の保管活動がある。TCMプロセスはツール製品が認証機関に受け入れられたときに終了せず、最終ソフトウェアのシステム又は環境のサービスライフを通して継続する。ツールライフサイクル活動がサプライヤにより実行されるときは、形態管理活動はサプライヤに適用されなければならない。

《7.2》

《7.2.1》形態識別(Configuration Identification)

活動には下記のものがある。

(a) 形態識別はツールライフサイクルデータのために確立されなければならない。
(b) 形態識別は各形態項目、形態項目の各々分離して管理される構成品、ツール製品を構成する形態項目の組み合わせのために確立されなければならない。
(c) 形態項目は変更管理やトレーサビリティ解析の実施より前に識別された形態でなければならない。
(d) 形態項目はその品目が他のツールライフサイクルプロセスで使用される又は他のライフサイクルデータから参照される前に識別された形態でなければならない。

《7.2.1》

《7.2.2》ベースラインとトレーサビリティ(Baselines and Traceability)

活動には下記のものがある。

(a) ベースラインは認証発行のために利用される形態項目のために確立されなければならない。(中間ベースラインはツールライフサイクルプロセス活動の管理を助力するために確立されるだろう。)
(b) ツール製品ベースラインはツール製品のために確立され、ツール形態索引内に定義されなければならない(10.1.11参照)。
(c) ベースラインはその完全性を確かにするために管理された(物理、電気又は他の)ソフトウェアライブラリ内に確立されなければならない。一度ベースラインが確立すると、それは変更から守られなければならない。
(d) 変更管理活動は確立されたベースラインからの派生ベースラインを開発するために継続されなければならない。
(e) もしツールライフサイクルプロセスの活動又は前のベースラインの開発に関連づけられたデータのために確認が求められるなら、ベースラインは派生元のベースラインに追跡可能でなければならない。
(f) もしツールライフサイクルプロセスの活動又は前の形態項目の開発と関連付けられたデータのために確認が求められるなら形態項目はそれが派生した形態項目から追跡可能でなければならない。
(g) ベースライン又は形態項目はそれが識別する成果物又はそれが関連するプロセスに追跡可能でなければならない。

《7.2.2》

《7.2.3》不適合報告、追跡、是正処置(Problem Reporting, Tracking, and Corrective Action)

活動には下記のものがある。

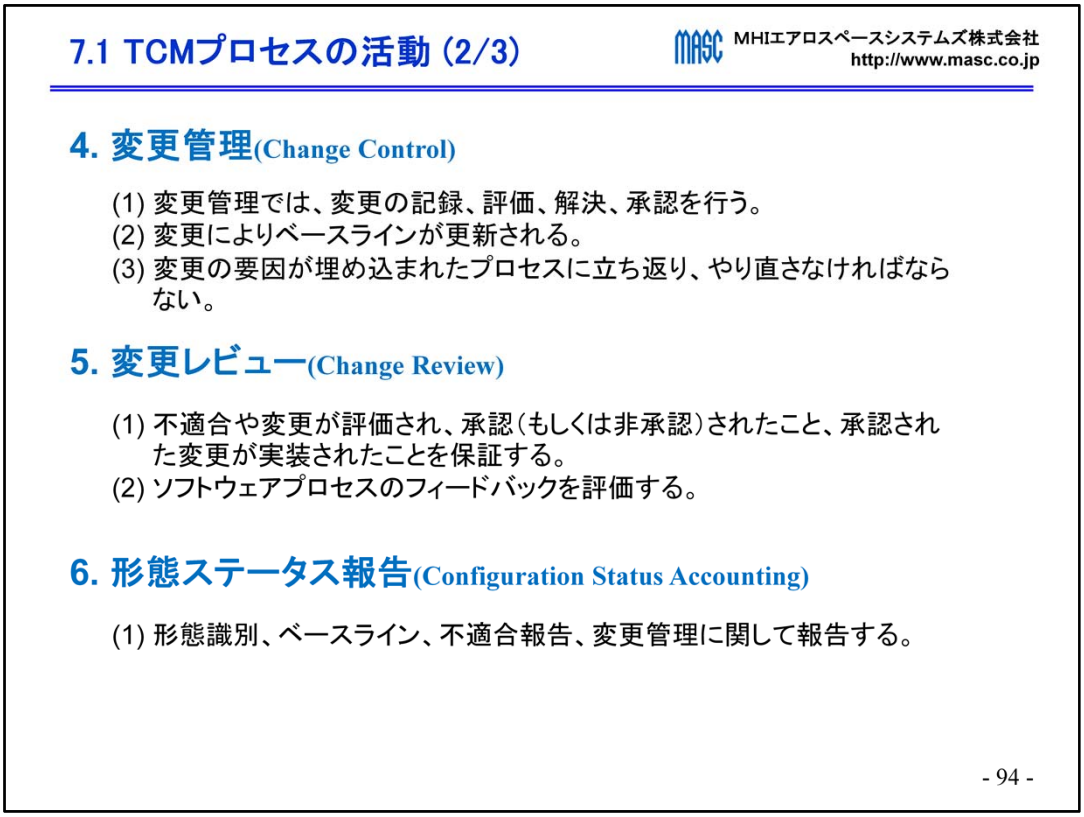
(a) ツール不適合報告は、10.1.12章に定義されたような計画へのプロセス不適合、成果物の欠如又はツール異常動作そして実施された是正措置が記述されるよう準備されなければならない。

Note:分離した不適合報告システムが利用されるかもしれない。例えば、ツール運用検証そして妥当性確認プロセスの間で検出されたエラーはツール検証プロセスの間で検出されたエラーとは別の不適合報告システムに記録されるかもしれない。

(b) 不適合報告は影響する形態項目の形態識別や影響するプロセス活動の定義、ツール不適合報告のステータス報告そしてツール不適合報告の承認と完了のために提供されなければならない。

(c) ツール製品又はツールライフサイクルプロセス成果物の是正措置を要求するツール不適合報告は変更管理活動を引き起こさなければならない。

《7.2.3》



【7.2】

4. 変更管理(Change Control)

変更管理の目的は、ツールライフサイクルを通して変更の記録、評価、解決、承認を行うものである。一旦、ベースライン化されたものは変更管理のプロセスを経由してのみ変更が許可される。前述の不適合報告と後述の変更レビューは変更管理と密接に関連しており、不適合報告がトリガーとなり変更管理が実行される。変更レビューは変更管理を支援するものである。

5. 変更レビュー(Change Review)

不適合管理に伴う変更、及び変更管理の結果を確認、評価するプロセスと位置づけられる。

6. 形態ステータス報告(Configuration Status Accounting)

報告先が不明だが、ツール形態管理プロセスの成果物であるツール形態管理記録(Tool Configuration Management Records)に残すことを意味しているのかもしれない。

《7.2.4》変更管理(Change Control)

活動には下記のものがある。

(a) 変更管理はその変更に対する保護を提供することで形態項目とベースラインの完全性を維持しなければならない。

(b) 変更管理は、形態項目に対するどのような変更もその形態識別子に対する変更を要求することを確認しなければならない。

(c) 派生ベースラインを製造するための変更管理下にあるベースラインと形態項目に対する変更は記録され、承認され、追跡されなければならない。不適合報告は、報告された問題の解決が結果として形態管理品又はベースラインの変更になりうるため、変更管理に関連付けられる。

Note:変更管理の早期の実行はツールライフサイクルプロセス活動の制御と管理を助けることは一般に知られている。

(d) ツール変更はその原点そしてその変更がその成果物に影響を与える点から続くツールライフサイクルプロセスを追跡できなければならない。例えば、不適切な設計の結果としてのエラーは設計の是正、コードの是正、インテグラルプロセスの活動の再開とならなければならない。

(e) 変更管理の間中、変更が影響するツールライフサイクルデータ更新され、記録は変更管理活動のために記録されなければならない。

変更管理活動は変更レビュー活動により補助される。

《7.2.4》

《7.2.5》変更レビュー(Change Review)

活動には下記がある。

(a) 全ての影響する形態項目が識別されているかの確認
(b) ツール運用要求への変更の影響の評価
(c) 実行される作業への判断を踏まえた不適合又は変更の評価
(d) ツール不適合報告又は変更の影響と影響するプロセスの決定によるフィードバックの提供
(e) ツールの不適合とツールプロセスが識別する提案された変更でのソフトウェアプロセスフィードバックの評価

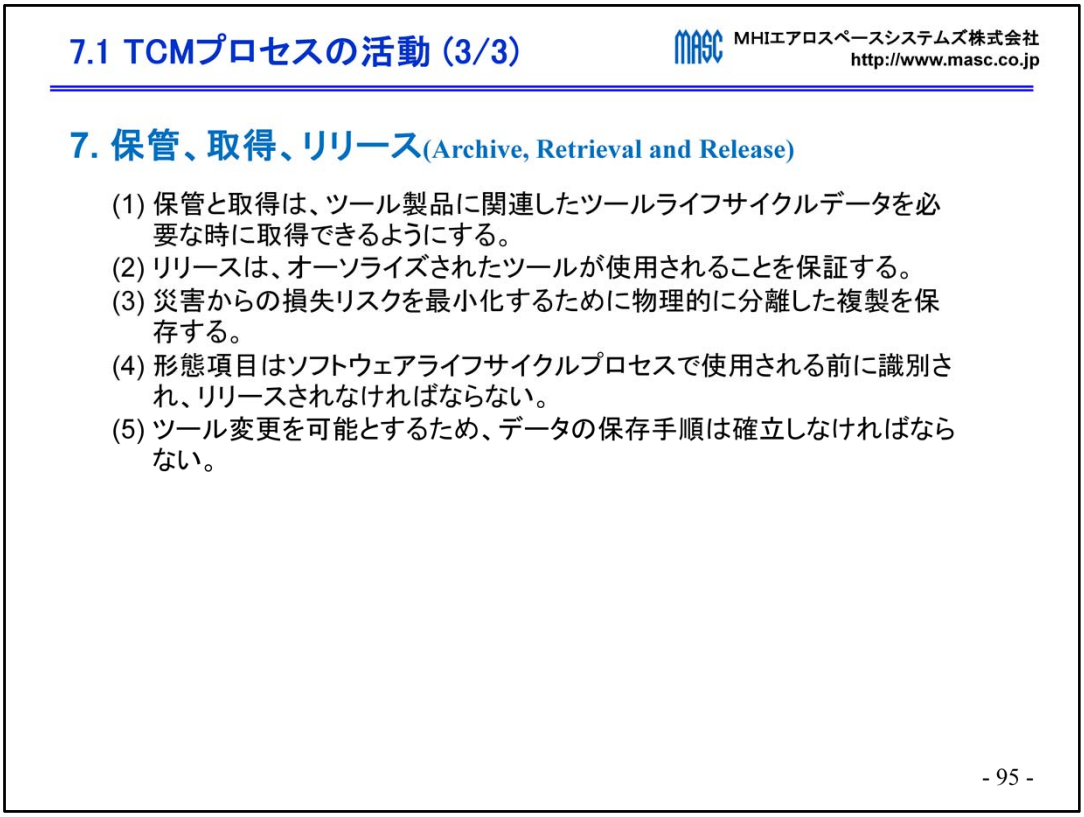
《7.2.5》

《7.2.6》形態ステータス報告(Configuration Status Accounting)

活動には下記がある。

(a) 形態項目の識別、ベースラインの識別、ツール不適合報告のステータス、変更履歴、リリースステータスの報告。
(b) 維持されるデータとデータのステータスの記録と報告の手段の定義

《7.2.6》



【7.2】

7. 保管、取得、リリース(Archive, Retrieval and Release)

ツールライフサイクルデータをどのように保管すべきかについて記載されている。
ベースラインを含めた形態項目が正しく識別され、間違いなくデータが複製される手段を提供しなければならない。また、ストレージメディアに関しても安全性を要求している。

《7.2.7》保管、回復、リリース(Archive, Retrieval, and Release)

活動には下記がある。

(a) ツール製品と関連するツールライフサイクルデータは承認されたソースから回復可能でなければならない(例えば、開発組織や会社での保管)。
(b) 手順は保管されたデータの完全性を確認するために手順は(保管先の媒体に関係なく)下記によって確立されなければならない。
    (1) 未承認の変更が反映されえないことの確認
    (2) 再生成によるエラーや悪化を最小化する保管媒体の選択
    (3) 時間経過による喪失や破損の防止。利用される保管媒体により、これは媒体の定期利用や保管データのリフレッシュを含む。
    (4) 災害発生時の紛失リスクを最小化するため、物理的に離れた保管所に重複した複製品の保管
(c) 正確な複製品の製造のため、複製プロセスは検証されなければならず、ツール実行可能オブジェクトコードのエラー無き複製を確認する手順が存在しなければならない。
(d) ソフトウェアライフサイクルプロセスでの利用に先んじて、形態項目は識別されリリースされなければならない。
(e) ツール変更を可能とするため、データ保持手順は確立されなければならない。

Note: 追加のデータ保持考慮事項は、この資料の範囲外であるビジネスニーズと将来の認証機関レビューの様な項を含むかもしれない。

《7.2.7》

7.2 TCMプロセスの目的

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
1	形態項目は識別されている。	7.1.a	7.2.1	○	○	○	○	○	ツール形態管理記録	10.1.3	②	②	②	②	②
2	ベースラインとトレーサビリティが確立されている。	7.1.b	7.2.2	○	○	○	○		ツール形態索引 ツール形態管理記録	10.1.11 10.1.13	① ②	① ②	① ②	① ②	
3	不適合報告、変更管理、変更レビュー、形態ステータス報告が確立されている。	7.1.c 7.1.d 7.1.e 7.1.f	7.2.3 7.2.4 7.2.5 7.2.6	○	○	○	○		ツール不適合報告 ツール形態管理記録	10.1.12 10.1.13	② ②	② ②	② ②	② ②	
4	保管、取得、リリースが確立されている。	7.1.g	7.2.7	○	○	○	○	○	ツール形態管理記録	10.1.3	②	②	②	②	②
5	ツールライフサイクル環境管理が確立されている。	7.1.h	7.4	○	○	○	○		ツール形態管理記録 ツールライフサイクル環境形態索引	10.1.13 10.1.10	② ①	② ①	② ①	② ②	

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

【Table T-8】

ツール形態管理プロセスは、他のツールライフサイクルプロセスと並行して実施され、以下の目的を実現する。

(1) ツールライフサイクル全体を通して、ツールの形態を定義する。
(2) 調査、改修が必要となった際に、実行可能オブジェクトコードの複製、再構築が可能な能力を提供する。
(3) ツールライフサイクルの各プロセスのインプットとアウトプットを管理する。これによりプロセスの一貫性を保証する。
(4) 形態項目とベースラインの設定により、レビュー、評価、変更管理のベースとなるポイントを提供する。
(5) 不適合や変更が記録され、承認され、修正されていることを保証できる仕掛けを提供する。
(6) ツールライフサイクルのアウトプットを管理することにより、ソフトウェアの承認のエビデンスを提供する。
(7) ツール製品が要求に準拠していることの評価を支援する。
(8) 形態項目が安全に物理的に保管され、リカバリ、管理が維持されていることを保証する。

《7.1》ツール形態管理プロセスの目的(Tool Configuration Management Process Objectives)

TCMプロセスの目的は下記である。

(a) 形態項目の管理と参照のための基礎を確立するため、各形態項目とその後継バージョンは明確に分類される。
(b) さらなるツールライフサイクルプロセス活動のためにベースラインは定義され、形態項目間の追跡可能性の管理と参照を許可する。
(c) 不適合報告プロセスはツール計画と標準と不一致のプロセスを記録し、ツールライフサイクルプロセスの成果物の不足を記録し、ツール製品の変則な挙動を記録し、これらの問題の解決を確かにする。
(d) 変更管理はツールライフサイクルを通して、記録、評価、解決、変更の承認を提供する。
(e) 変更レビューは問題と変更が評価され、問題と変更が承認又は棄却され、承認された変更が実行され、ツール計画プロセスの間に定義された不適合報告及び変更管理手法を通してフィードバックが影響するプロセスに提

供されることを確かにする。

(f) ステータス報告は形態識別、ベースライン、不適合報告、変更管理に関してツールライフサイクルプロセスの形態管理のためのデータを提供する。

(g) ツール製品の複製、再生成、再試験又は改修の必要がある際に、保管と取得はツール製品に関連したツールライフサイクルデータが取得できることを確認する。リリース活動の目的はソフトウェアライフサイクルプロセスで承認されたツールのみが利用されることを確認することである、加えて保管と取得されることを確認する。

(h) ツールライフサイクル環境管理はツール自身の製造に利用される他のツールが識別され、管理され、取得できることを確かにする。

TCMのための目的はTQLから独立している。しかしながら、二つのカテゴリのツールライフサイクルデータは、データに適用されるTCM管理を基に存在しているだろう(7.3参照)。

付録Aの表T-8はTQLごとのTCMプロセスの目的と成果物の概要である。

《7.1》

7.3 形態管理カテゴリ

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

No	ソフトウェア形態管理項目	CC1	CC2
1	Configuration Identification	○	○
2	Baselines	○	
3	Traceability	○	○
4	Problem Reporting	○	
5	Change Control - integrity and identification	○	○
6	Change Control - tracking	○	
7	Change Review	○	
8	Configuration Status Accounting	○	
9	Retrieval	○	○
10	Protection against Unauthorized Changes	○	○
11	Media Selection, Refreshing, Duplication	○	
12	Release	○	
13	Data Retention	○	○

- 97 -

【7.3】

DO-330ではツールライフサイクルデータの形態管理の方法を厳密に定義している。

この表は前述したツール形態管理プロセスで定義された13の形態管理項目を示している。

CC1は「Control Category 1」、CC2は「Control Category 2」の略である。

本資料では、「Control Category」を「形態管理カテゴリ」と訳している。

DO-330では、ツールレベル(TQL1～TQL5)に応じてツールライフサイクルデータの形態管理のレベル(CC1、CC2)を定めている。

CC1が指定されると１３項目の全ての形態管理項目を実施する必要がある。CC2が指定された場合は、表で○のついた項目だけを最低限実施すればよい。

《7.3》データ管理カテゴリ(Data Control Categories)

ツールライフサイクルデータは二つの分類：形態管理カテゴリ1(CC1)と形態管理カテゴリ2(CC2)の一つに割り当てることができる。

これらの分類はデータの形態管理制御に関連付けられる。

表7-1は各管理カテゴリに関連付けられたTCMプロセス活動群を定義する、そこでは●がその分類のツールライフサイクルデータに活動を適用することを示す。

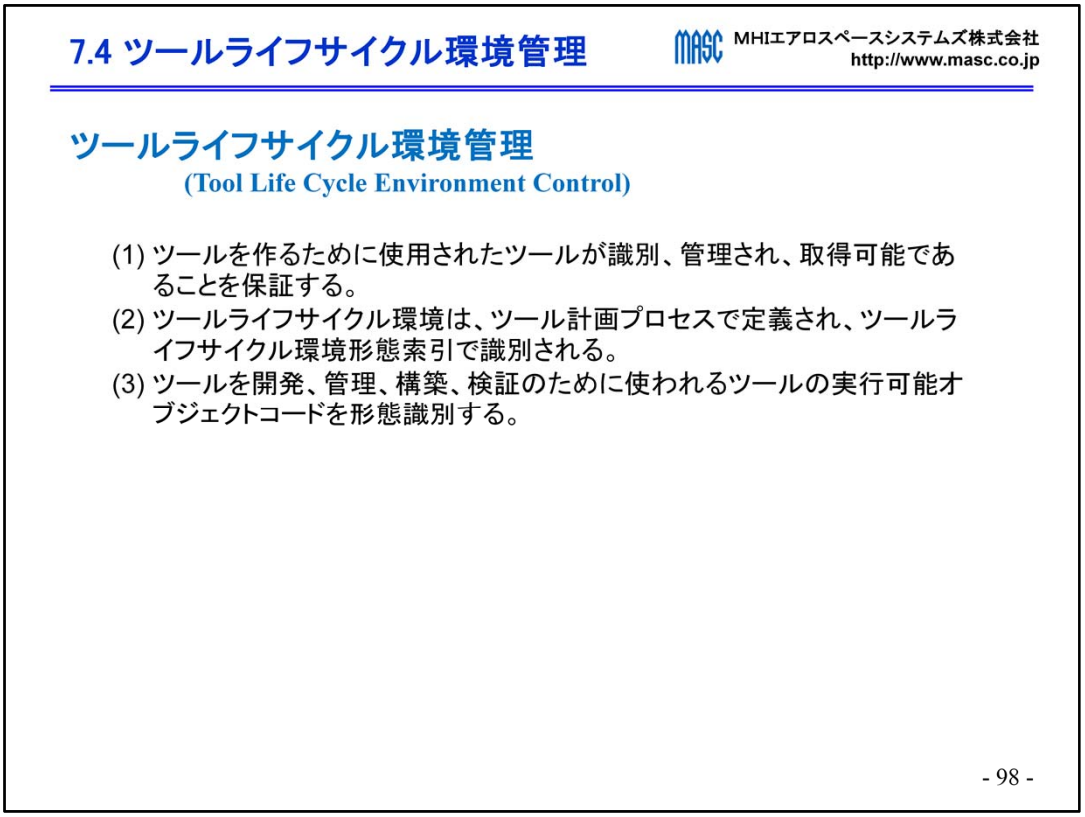
CC2活動はCC1活動の部分集合である。

付録Aの表は、TQL毎に各ツールライフサイクルデータアイテムの形態管理カテゴリを明記する。データ管理カテゴリのガイダンスには下記があげられる。

(a) CC1に分類されたツールライフサイクルデータのためのTCMプロセス活動は表7-1に従って適用されなければならない。

(b) CC2に分類されたツールライフサイクルデータのためのTCMプロセス活動は、最低限として、表7-1に従って適用されなければならない。

《7.3》



【7.4】

7.4 ツールライフサイクル環境管理

ここでは、ツールを作成するために使用されたツールの形態管理について規定している。

ツールライフサイクルデータを形態管理することはもちろんであるが、ツールライフサイクルプロセスで使用された環境（ツール）に関しても形態管理される必要がある。ツールライフサイクルデータは再構築可能でなければならず、そのためにはその時に使用した環境が特定でき、環境自体も再構築可能でなければならないからである。

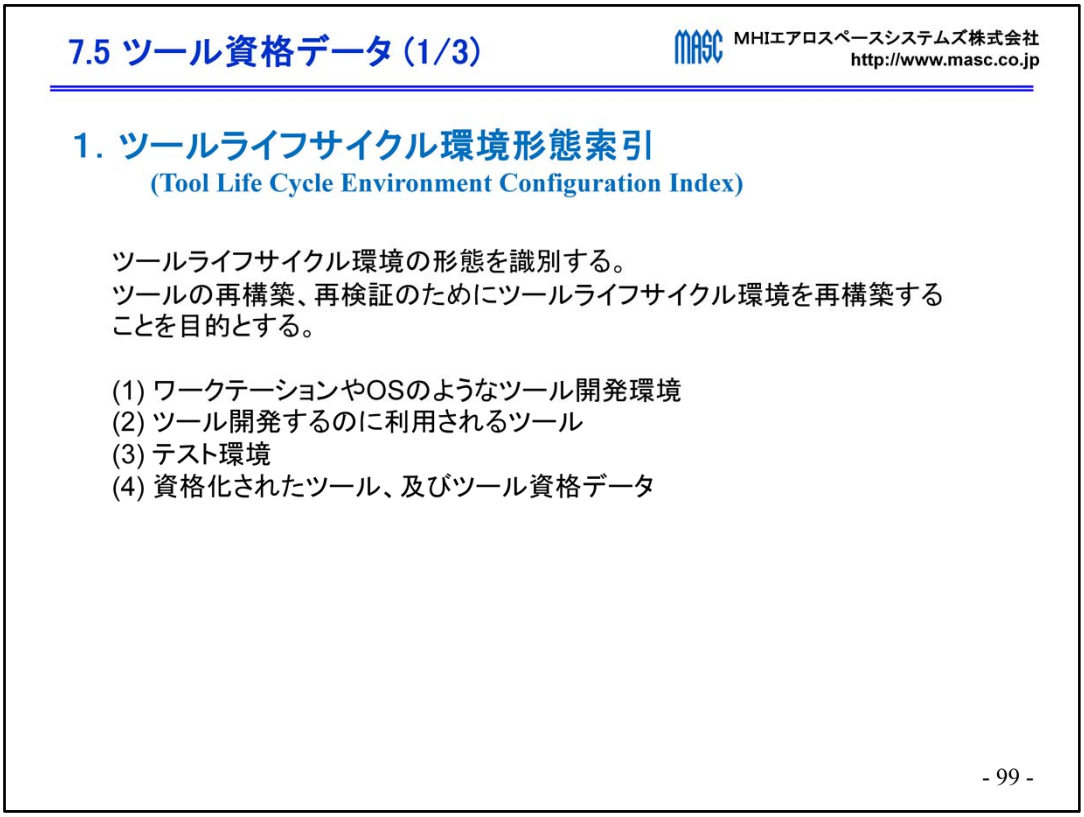
《7.4》ツールライフサイクル環境管理 (Tool Life Cycle Environment Control)

ツールライフサイクル環境はツール計画プロセスにより定義され、ツールライフサイクル環境形態索引(10.1.10参照)により識別される。活動には下記があげられる。

(a) 形態識別子は、開発、管理、ビルド又はツール製品とそのデータの検証に利用されるツールの実行可能オブジェクトコード(又は同等のもの)のために確立されなければならない。

(b) ツール実行オブジェクトコード(又は同等のもの)の製造に利用されるツール(例えば、コンパイラ、アセンブラ、リンケージエディタ)を管理するTCMプロセスは最低限CC2に関連した目的に準拠せねばならない。

《7.4》



【10.1.10】

《10.1.10》ツールライフサイクル環境形態索引(Tool Life Cycle Environment Configuration Index)

ツールライフサイクル環境形態索引はツールライフサイクル環境の形態を識別する。

この索引は、実行可能コードの再製造やツール再検証又は変更のためにツール開発や検証環境の再製造を支援するために記述される。

索引は下記を実施しなければならない。

(a) 例えばワークステーションやOSのようなツール開発環境を識別する。

(b) 認証のために提出されるツールを開発するのに利用されるツールを識別する。(例えば、コンパイラやリンケージエディタ)

(c) もしツール開発環境と異なれば、ツール検証環境を識別する。

(d) 認証ツールとその関連するツール資格データを識別する。これらのツールは認証のために提出されるツールのライフサイクルプロセスのコンテキスト内で利用されるものである。

《10.1.10》

7.5 ツール資格データ(2/3)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

2. ツール形態索引(Tool Configuration Index)

ツール製品の形態を識別する。以下が特定されなければならない。

(1) ツール製品
(2) 関連する全てのファイルを含むツール実行可能オブジェクトコード
(3) 各ツールソースコード
(4) 既開発コンポーネント
(5) ツールライフサイクルデータ
(6) ツールライフサイクル環境形態索引への参照
(7) 保管、リリースメディア
(8) ツール実行可能オブジェクトコードのビルドのための説明書

- 100 -

【10.1.11】

《10.1.11》ツール形態索引 (Tool Configuration Index)

ツール形態索引はツール製品の形態を識別する。特別な形態識別やバージョン識別が提供されなければならない。

ツール形態索引は下記を識別しなければならない。

(a) ツール製品
(b) 関連するすべてのファイルを含むツール実行可能オブジェクトコード
(c) 各ツールソースコードコンポーネント
(d) もし利用するなら、ツール製品内で既開発のコンポーネント
(e) ツールライフサイクルデータ
(f) もし分けて纏められるなら、ツールライフサイクル環境形態索引(10.1.10参照)への参照
(g) 保管とリリースの媒体
(h) ツール実行可能オブジェクトコードのビルドのための説明書(例えば、コンパイルやリンクのための指示やデータのようなアイテムを含む) と再製造、テスト、変更のためにツールを回復するのに利用される手順

備考1:ツール形態索引は一つ又はセット(階層)のデータアイテムを含むことができる。ツール形態索引は上記に示されたアイテムを含むことができる、もしくは、他のツール形態索引を参照するかもしれない、又は各アイテムとそのバージョンを特定する形態データを識別する。

備考2:ツール形態索引は一つのツール製品バージョンのために作成されるだろうもしくは、いくつかの代替え又は後継ツール製品バージョンのためのデータを含むために拡張されるだろう。

備考3：ツール形態索引はツール開発プロセス間に製造されたデータのみを含むだろう。それはツール運用環境内で統合されたツール全てのデータを識別しないだろう。この場合、ツールを利用するソフトウェアのためのソフトウェアライフサイクル環境形態索引はそのデータを識別しなければならない。

《10.1.11》

7.5 ツール資格データ(3/3)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

3. ツール不適合報告(Tool Problem Reports)

ツール製品とプロセスの不適合を記録する。

(1) 不適合が発見された形態項目、もしくはプロセス
(2) 変更された形態項目、プロセス
(3) 不適合の説明
(4) 是正処置内容

4. ツール形態管理記録 (Tool Configuration Management Records)

ツール形態管理プロセスの結果を記録する。

(1) 形態識別リスト
(2) ベースライン
(3) 変更履歴報告
(4) 保管記録
(5) リリース記録

- 101 -

【11.17】

3. ツール不適合報告(Tool Problem Reports)

《10.1.12》ツール不適合報告 (Tool Problem Reports)

ツール不適合報告は、ツール製品の特異な動作や、ツール計画や標準に準拠しないプロセス、ツールライフサイクルデータの欠陥の解決を識別し記録する手法である。ツール不適合報告は下記を含まなければならない。

(a) 問題が観測された形態項目やツールライフサイクルプロセス活動の識別
(b) 変更される形態項目の識別又は変更されるプロセスの説明
(c) 問題が理解され解決されるようにする問題説明
(d) 報告された問題を解決するためにとられた是正措置の説明

《10.1.12》

【11.18】

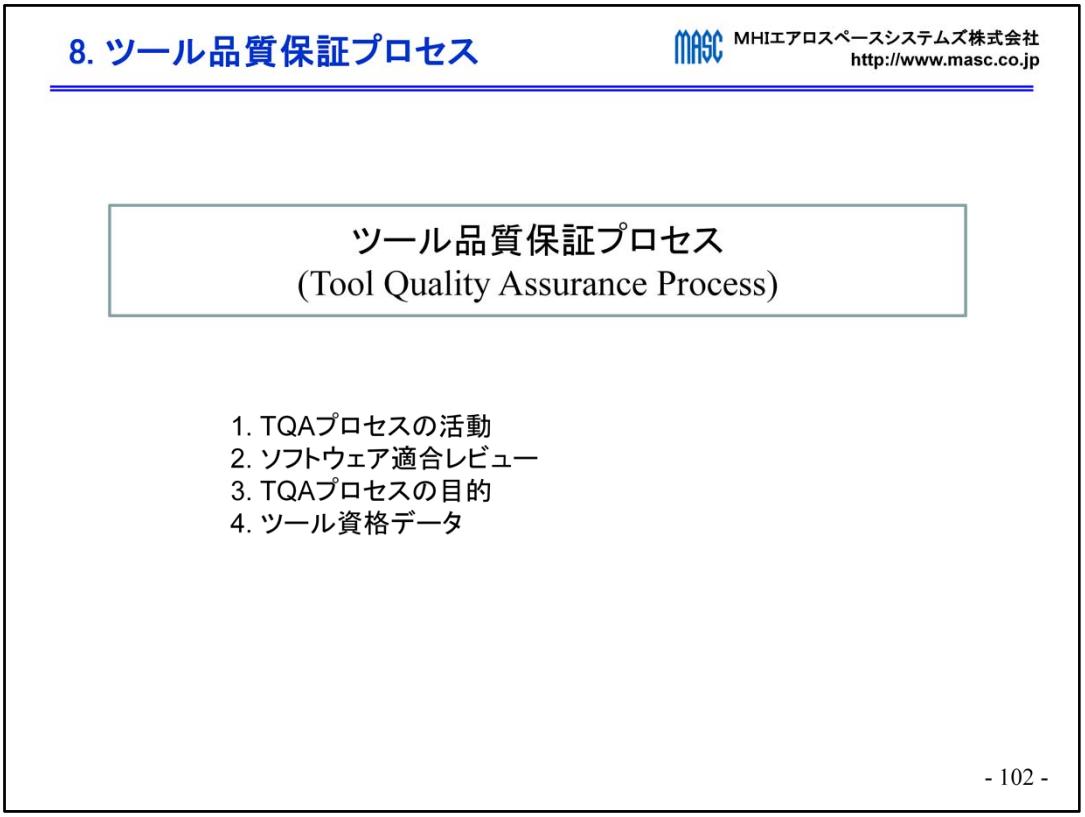
4. ツール形態管理記録(Tool Configuration Management Records)

《10.1.13》ツール形態管理記録 (Tool Configuration Management Records)

TCMプロセス活動の結果はTCM記録に記録される。例には形態識別リスト、ベースライン、変更履歴報告、保管記録、リリース記録がある。これらの例は、これら特別な形式の記録を作成する必要性を示すものではない。

備考:TCMプロセスの統合的特性に従い、その成果物は他のライフサイクルデータの一部としてしばしば含まれるだろう。

《10.1.13》



【8】

ツール品質保証プロセスは、承認された計画と標準に従ってプロセスが実行されていることを保証するものであり、それによりツールライフサイクルプロセスが要求に適合したツールを作成していることを保証するものである。

《8.0》ツール品質保証プロセス(Tool Quality Assurance Process)

この章ではツール品質保証(TQA)プロセスの目的と活動について説明する。TQAプロセスはツール計画プロセス(4章)とツール品質保証計画(10.1.6参照)で定義された通りに適用される。TQAプロセス活動の成果物はツール品質保証記録(10.1.14参照)又は他のツールライフサイクルデータに記録される。

TQAプロセスは下記の保証を得るためツールライフサイクルプロセスとその成果物を評価する。

(a) 目的は満たされている。
(b) 欠陥は検出され、評価され、追跡され、解決される。
(c) ツール製品とツールライフサイクルデータはこの資料ともしあれば追加の規則要求を確認する。

《8.0》

8.1 TQAプロセスの活動

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

以下を保証する。

(1) TQAプロセスは、権威、責任、独立を持って実行されなければならない。
(2) ツール計画と標準に一貫性があり、レビューされている。
(3) ツールライフサイクルプロセスが承認された計画と標準に準拠している。
(4) ツール開発、及びインテグラルプロセスの監査。
(5) ツールライフサイクルプロセスの移行基準が承認されたツール計画に準拠している。
(6) ツールライフサイクルデータがコントロールカテゴリに従い管理されている。
(7) ツール適合レビュー(Tool Conformity Review)が実施されている。
(8) TQAプロセス活動の記録の作成。

- 103 -

【8.2】

《8.2》ツール品質保証プロセスの活動 (Tool Quality Assurance Process Activities)

TQAプロセスの目的を満たす活動には下記のものがある。

(a) TQAプロセスを実施する者はツールライフサイクルプロセスの活動において積極的な役割を担い、TQAプロセスの目的が満たされることを確実にするための権限、責任そして独立性を持たなければならない。

(b) TQAプロセスはツール計画と標準が開発され一貫性のためにレビューされる保証を与えなければならない。

(c) TQAプロセスはツールライフサイクルプロセスが承認されたツール計画と標準に準拠する保証を与えなければならない。

(d) TQAプロセスは下記の保証を得るためツールライフサイクルの間にツール開発とインテグラルプロセスの審査を含まなければならない。

(1) ツール計画は4章に規定された通りに入手できる。

(2) ツール計画と標準からの逸脱が検出、記録、評価、追跡、解決される。

備考:プロセス逸脱の早期検出はツールライフサイクルプロセス目的の効果的な達成を補助すると一般的に認められている。

(3) 承認された逸脱は記録される。

(4) ツール開発環境はツール計画で規定された通りに提供されている。

(5) 不適合報告、追跡、是正措置プロセスがツール形態管理計画に準拠している。

備考:ツールライフサイクルプロセスの活動の監視は、活動が管理下にある保証を提供するために実施されるかもしれない。

(e) TQAプロセスはツールライフサイクルプロセスの移行基準が承認されたツール計画に準拠して満たされている保証を与えなければならない。

(f) TQAプロセスは、ツールライフサイクルデータが7.3章と付録Aの表に規定された管理カテゴリに従った管理下にある保証を与えなければならない。

(g) 認定申請の一部として提出される最終ソフトウェアにより利用されることが意図されたツール製品の配布前にツール適合レビューは実施されなければならない。

(h) TQAプロセスはTQAプロセス活動の記録(10.1.14参照)を作成しなければならない。記録は各ツールに対する審査結果とツール適合レビュー完了の証拠を含む。

(i) TQAプロセスは、いかなるサプライヤプロセスと成果物が承認されたツール計画と標準に準拠している保証を与えなければならない。

《8.2》

8.2 ツール適合レビュー

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

ツール製品について、ツールライフサイクルプロセスが完了し、ツールライフサイクルデータが作られ、ツール実行可能オブジェクトコードが管理され、再構築可能であることを保証するためのレビューを実施する。

(1) ツールライフサイクルプロセスは完了している。
(2) ソフトウェアライフサイクルデータは作成されている。
(3) ツールライフサイクルデータがTCM計画通りに管理されている。
(4) ツール不適合報告が正しく管理され、記録されている。
(5) ツール要求のデビエーションが記録され、承認されている。
(6) ツール実行可能オブジェクトコードがソースコードから再構築可能である。
(7) 以前のツール適合レビューからの不適合報告は再評価されている。
(8) 現ツールのベースラインは以前のベースラインからトレース可能である。

- 104 -

【8.3】

《8.3》ツール適合レビュー(Tool Conformity Review)

ツール適合レビューの目的は、ツール製品に対しツールライフサイクルプロセスとデータが完全で、ツール実行可能オブジェクトコードが管理され再生成可能である保証を得ることである。

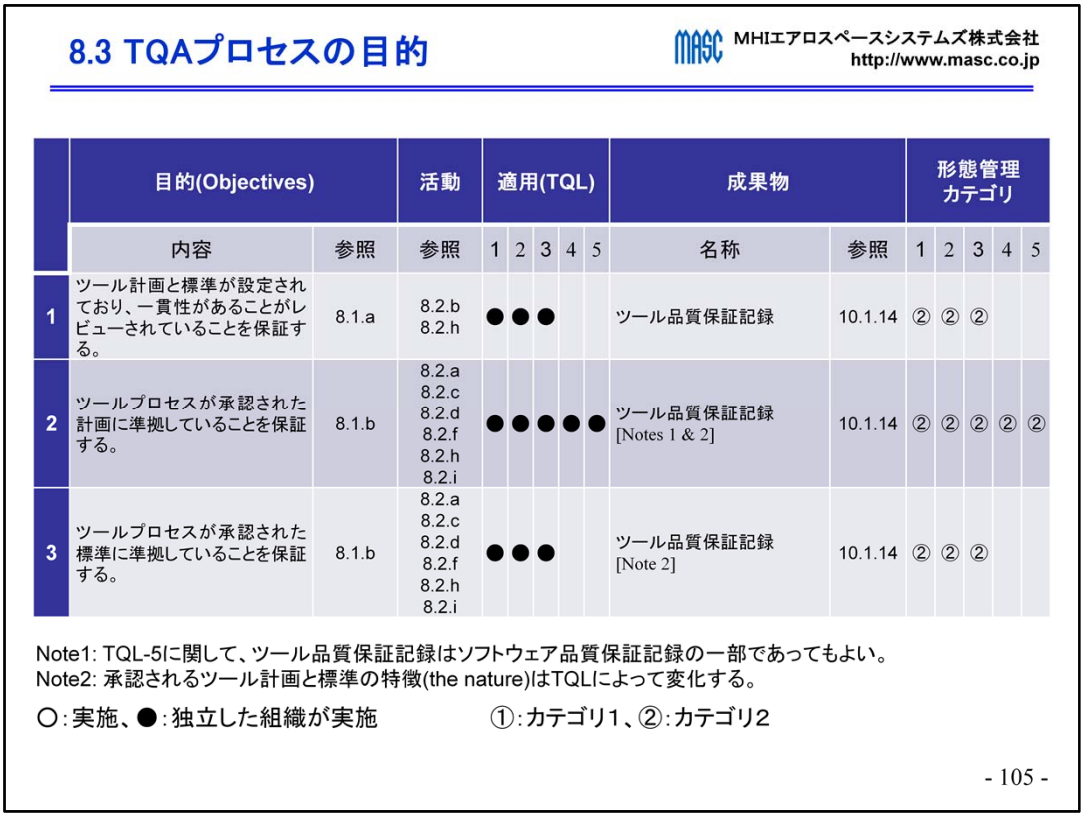
ツール適合レビューはソフトウェア適合レビューのコンテキスト内で実行又は補足されるだろう。

このレビューは下記を決定しなければならない。

(a) ツールライフサイクルデータの製造を含む計画されたツールライフサイクルプロセス活動は完了し、その完了記録は保管されている。
(b) ツールライフサイクルデータがツール計画と標準に従い生成され、TCM計画に従い管理されている証拠が存在する。
(c) ツール不適合報告が評価されそのステータスが記録されている証拠が存在する。
(d) ツール要求逸脱が記録され承認されている。
(e) ツール実行可能オブジェクトコードが保管されたツールソースコードから再生成可能である。
(f) 前回のツール適合レビューから保留されているツール問題報告がそのステータスを決定するために再評価されている。
(g) 認証発行が既開発のツールの仕様を求めるのであれば、現在のツール製品のベースラインは前のベースラインとそのベースラインへの承認された変更へ追跡可能である。

備考:過去の認定ツールの変更のため、ツール適合レビュー活動の変更の重要度により正当化されたサブセットが実行されるかもしれない。

《8.3》



8.3 TQAプロセスの目的

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
1	ツール計画と標準が設定されており、一貫性があることがレビューされていることを保証する。	8.1.a	8.2.b 8.2.h	●	●	●			ツール品質保証記録	10.1.14	②	②	②		
2	ツールプロセスが承認された計画に準拠していることを保証する。	8.1.b	8.2.a 8.2.c 8.2.d 8.2.f 8.2.h 8.2.i	●	●	●	●	●	ツール品質保証記録 [Notes 1 & 2]	10.1.14	②	②	②	②	②
3	ツールプロセスが承認された標準に準拠していることを保証する。	8.1.b	8.2.a 8.2.c 8.2.d 8.2.f 8.2.h 8.2.i	●	●	●			ツール品質保証記録 [Note 2]	10.1.14	②	②	②		

Note1: TQL-5に関して、ツール品質保証記録はソフトウェア品質保証記録の一部であってもよい。
Note2: 承認されるツール計画と標準の特徴(the nature)はTQLによって変化する。

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

- 105 -

【Table T-9】

《8.1》ツール品質保証プロセスの目的(Tool Quality Assurance Process Objectives)

TQAプロセスの目的は、承認されたツール計画や規則に従ってこれらのプロセスが実施されたことを保証することによりその要求を確認するツールをツールライフサイクルプロセスが製造することに確信を与える。

TQAプロセスの目的は下記を実施することである。

(a) ツール開発計画と標準が開発され一貫性のためにレビューされる保証の獲得
(b) ツール開発プロセスとインテグラルプロセス(サプライヤのそれらを含む)が承認されたツール計画と標準に準拠する保証の獲得
(c) ツールライフサイクルプロセスの移行条件が満たされている保証の獲得
(d) ツール製品の適合レビューの実施

TQLごとの目的の適用性は付録Aの表T-9に規定する。

《8.1》

8.3 TQAプロセスの目的

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
4	ツールライフサイクルプロセスの移行基準が満足していることを保証する。	8.1.c	8.2.e 8.2.h	●	●	●			ツール品質保証記録	10.1.14	②	②	②		
5	ツールの適合レビューが実施されていることを保証する。	8.1.d	8.2.g 8.2.h 8.3	●	●	●	●	●	ツール品質保証記録 [Notes 1]	10.1.14	②	②	②	②	②

Note1: TQL-5に関して、ツール品質保証記録はソフトウェア品質保証記録の一部であってもよい。
Note2: 承認されるツール計画と標準の特徴(the nature)はTQLによって変化する。

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

- 106 -

【Table T-9】

8.4 ツール資格データ

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

1. ツール品質保証記録 (Tool Quality Assurance Records)

TCMプロセス活動の結果を記録する。

(1) TQAレビュー
(2) 監査報告
(3) 会議議事録
(4) 許可されたプロセスの逸脱の記録
(5) ツール適合レビューの結果

- 107 -

【10.1.14】

《10.1.14》ツール品質保証記録 (Tool Quality Assurance Records)

TQAプロセス活動の結果はTQA記録に記録される。これらはTQAレビュー、監査記録、会議議事録、認可されたプロセス逸脱の記録、ツール適合レビュー記録を含むだろう。

ツールの開発を取り扱うTQA記録に加えて、その利用を取り扱うソフトウェア品質保証記録があるだろう。

《10.1.14》

【9】

ツール認証連絡プロセスは、認証プロセスを支援するためにツールライフサイクルを通して、申請者と認証機関との間のコミュニケーションと理解を確立する。

ツール認証連絡プロセスは単独で実施されず、ソフトウェアの認証連絡プロセスのフレームワークにある。

《9.0》ツール認証連絡プロセス (Tool Qualification Liaison Process)

ツール認証連絡プロセスは単独で実施されない、しかしソフトウェアの認証連絡プロセス(又は同等、ドメインに依存する)のフレームワークにある。この章はこのプロセスのツール認証の特徴を明確にする。

認証機関との連絡はツール認証のために必要とされる。PSACはソフトウェアライフサイクルプロセス内のツールの特定利用によるツール認証の必要性を識別する。

ソフトウェアライフサイクルプロセス内で、1つ以上のツールが認証されることが必要とPSACが識別した場合、認証連絡プロセスには次の活動があげられる。

(a) 認証機関に送付される主な入力はツール認証識別を含むPSACである。認証機関に送付されなければならない最低限のデータは下記である。
- ・認証ソフトウェアの概要計画(PSAC)
- ・ツール認証計画(TQP)
- ・ツール形態索引(TCI)
- ・ツール完了報告(TAS)
- ・ソフトウェアライフサイクル形態索引(SECI)
- ・ソフトウェア完了報告(SAS)

TQL-5について、TQP、TCIそしてTASは要求されない。

(a) PSACとTQPの両方は認証機関に適合の手段の合意を得るために送付されなければならない。

(b) ツールライフサイクルプロセスが計画を満たす証拠のように、ツールライフサイクルデータはレビューのために認証機関へ利用可能でなければならない。

(c) 全ての既知の問題と機能的制限はソフトウェアライフサイクルプロセスの観点から分析されなければならず、ソフトウェア完了報告の中で報告が提供されなければならない。ツールの機能と出力がツール運用要求に従うことを確認するためにツールの既知の問題と機能的制限の影響は識別され、解析されなければならない。

(d) ソフトウェアライフサイクル環境形態索引は、適切なソフトウェアリリースの範囲内で利用されるすべてのツールの識別を提供しなければならない。TQL-5では、それはツール認証データへの参照も含まなければならない (ツール運用要件、ツール運用検証妥当性データ) 。他のTQLでは、ソフトウェアラウフサイクル環境形態索引はTCIを参照しなければならない。

《9.0》

9.1 ツール認証計画プロセスの活動 (1/2)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

ソフトウェアライフサイクルプロセスで、ツールが資格化が必要とPSACが識別した場合、次の活動があげられる。

(1) 認証機関へデータの提出。提出する最低限のデータは以下である。
  a. ソフトウェア認証計画(PSAC)
  b. ツール認証計画(TQP)
  c. ツール形態索引(TCI)
  d. ツール完了報告(TAS)
  e. ソフトウェアライフサイクル環境形態索引(SECI)
  f. ソフトウェア完了報告(SAS)

  ただしTQL-5について、TQP, TCI, TASは要求されない。

(2) PSACとTQPに関して認証機関の同意を得る
(3) ツールライフサイクルプロセスが計画を満たす証拠として、ツールライフサイクルデータはレビューのために認証機関に利用可能でなければならない

- 109 -

【9.0】

9.1 ツール認証計画プロセスの活動 (2/2)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

(4) もしツールの既知の問題と機能的制限がある場合、ソフトウェアライフサイクルプロセスの観点から分析され、ソフトウェア完了報告の中で報告されなければならない。また、ツールの機能と出力がツール運用要求(Tool Operational Requirements)に従うことを確認するために、ツールの既知の問題と機能的制限の影響は識別され、解析されなければならない。

(5) ソフトウェアライフサイクル環境形態索引(SCEI)は、適切なソフトウェアリリースの範囲内で利用される全てのツールの識別を提供しなければならない。

9.3 ツール認証連絡プロセスの目的

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

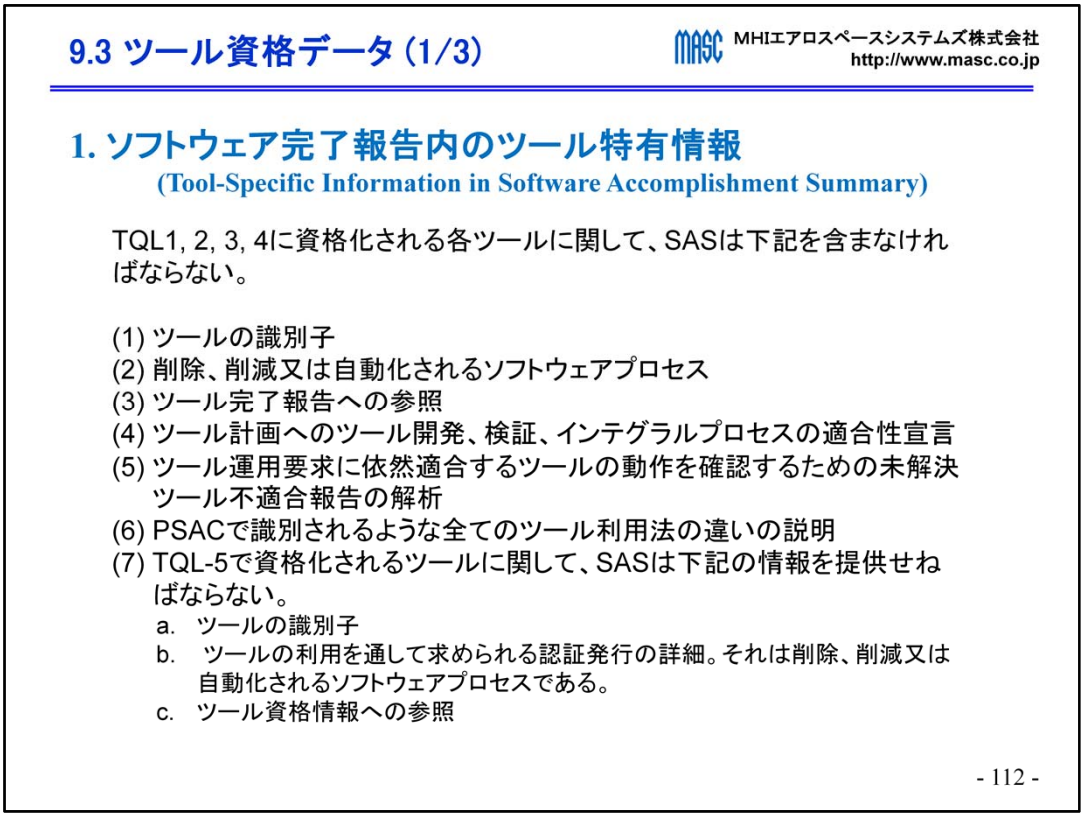
	目的(Objectives)		活動	適用(TQL)					成果物		形態管理カテゴリ				
	内容	参照	参照	1	2	3	4	5	名称	参照	1	2	3	4	5
1	申請者と認証機関との間でコミュニケーションと理解を確立する。	9.0	9.0.a	○	○	○	○	○	PSAC内のツール固有情報	10.1.1	①	①	①	①	①
									ツール資格計画 [Note 1]	10.1.2	①	①	①	①	①
2	遵守の方法が提案され、同意が取れている。	9.0	9.0.b	○	○	○	○	○	PSAC内のツール固有情報	10.1.1	①	①	①	①	①
									ツール資格計画 [Note 1]	10.1.2	①	①	①	①	①
3	遵守の実証が提供されている。	9.0	9.0.c 9.0.e	○	○	○	○	○	ソフトウェア完了報告内のツール特有情報	10.1.16	①	①	①	①	①
									ツール完了報告[Note 2]	10.1.15	①	①	①	①	①
									ソフトウェアライフサイクル形態索引内のツール特有情報	10.1.17	①	①	①	①	①
									ツール形態索引 [Note 3]	10.1.11	①	①	①	①	①
4	ツール運用環境における既知の問題の影響が識別され分析されている。	9,0	9.0d	○	○	○	○	○	ソフトウェア完了報告内のツール特有情報	10.1.16	①	①	①	①	①

Note1: TQL-5に関して、この項目はソフトウェア認証計画(PSAC)によって満たされても良い。
Note2: TQL-5に関して、この項目はソフトウェア完了報告(SAS)によって満たされても良い。
Note3: TQL-5に関して、この項目はソフトウェアライフサイクル環境形態索引(SECI)によって満たされても良い。

○:実施、●:独立した組織が実施　　①:カテゴリ1、②:カテゴリ2

- 111 -

【Table T-10】



【10.1.16】

《10.1.16》ソフトウェア完了報告内のツール特有情報(Tool-Specific Information in PSAC)

TQL1、2、3、4に認定される各ツールのため、SASは下記を含まなければならない。

(a) ツールの識別子

(b) ツールの利用を通して求められる認証確認の詳細、それは削除、削減又は自動化されるソフトウェアプロセスである。

(c) ツール完了報告への参照

(d) ツールユーザの活動を含むツール計画へのツール開発、検証、インテグラルプロセスの適合性宣言

(e) ツール運用要求に依然適合するツールの動作を確認するための未解決ツール不適合報告の解析

(f) PSACで識別されるような全てのツール利用法の違いの説明

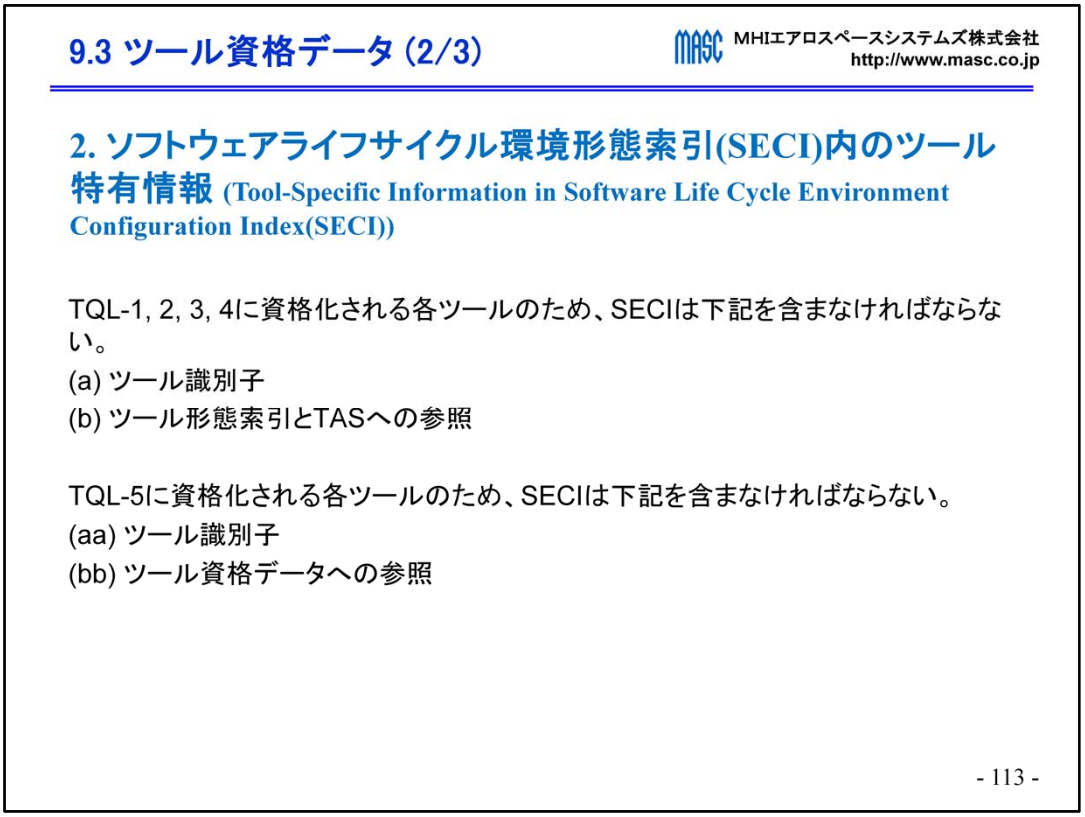
(g) TQL-5に認定されるツールのために、SASは下記の情報を提供せねばならない。

(1) ツールの識別子

(2) ツールの利用を通して求められる認証確認の詳細、それは削除、削減又は自動化されるソフトウェアプロセスである。

(3) ツール資格情報への参照

《10.1.16》



【10.1.17】

《10.1.17》ソフトウェアライフサイクル環境形態索引(SECI内)のツール特有情報

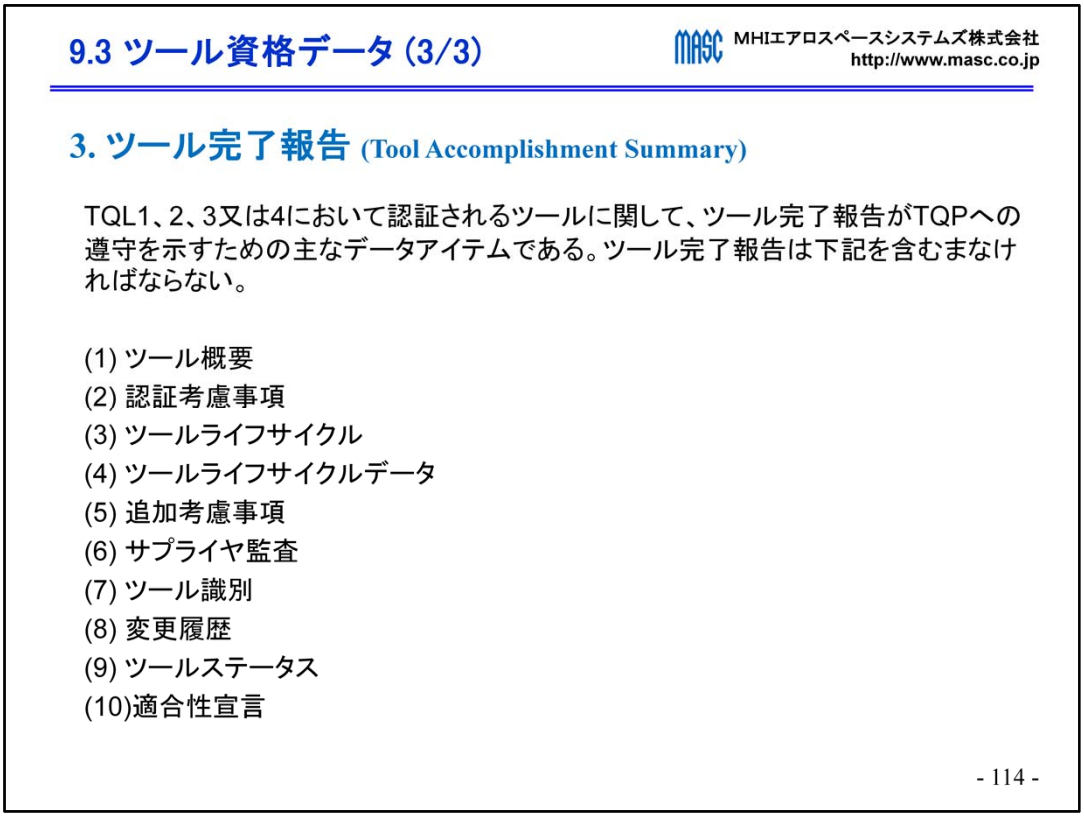
TQL1、2、3、4に認定される各ツールのため、SECIは下記を含まなければならない。

(a)　ツールの識別子
(b)　ツール形態索引とTASへの参照

TQL5に認定される各ツールのため、SECIは下記を含まなければならない。

(aa) ツールの識別子
(bb) ツール資格情報への参照

《10.1.17》



【10.1.15】

TQL-5の場合、ツール完了報告の内容はソフトウェア完了報告(SAS)に記載されても良い。

《10.1.15》ツール完了報告(Tool Accomplish Summary)

TQL1、2、3又は4において認証されるツールには、ツール完了報告がTQPへの遵守を示すための主なデータアイテムである。

ツール完了報告は下記を含まなければならない。

(a) ツール概要

この項はツールの主な機能、その入力と出力、TQPで提案されたツール概要からの全ての違いを簡潔に説明する。

(b) 認証考慮事項

この項はTQPで説明されたツールのために提案されたTQLを再記述する。それは運用環境も識別する。

(c) ツールライフサイクル

この項は、実際のライフサイクルを要約し、TQPで識別されたツール資格活動からの違いを説明する。

(d) ツールライフサイクルデータ

作成されたツールライフサイクルデータ、データ間とツールを定義する他のデータとの関係、認証機関がデータを利用可能にする手段のため、この項はTQPで作成された提案からのすべての違いを記述する。この項は形態識別子とバージョン毎に、適合するツール形態索引、ツールライフサイクル環境索引を明確に参照する。ツールライフサイクル内の形態識別子と特定のバージョンに関する詳細な情報はツール形態索引により提供される。

(e) 追加考慮事項

この項は認証機関の注意に値するであろう認証の論点を要約する。そのような懸念に関するTQPに含まれる提案からのすべての違いをそれは説明する。特別な条件や説明資料などの適切なデータアイテムへの参照が作られなければならない。

(f) サプライヤ監査

この項はどのようにサプライヤプロセスと成果物が承認された計画や標準に従うかを説明する。

(g) ツール識別

この項は部品番号とバージョン毎のツール形態を識別する。

(h) 変更履歴

該当する場合、この項は前回の認証からの、ツール機能に影響を与える変更の概要を含み、ツールライフサイクルプロセスからの全ての変更又は改善を識別する。

(i) ツールステータス

この項は、承認時に未解決のツール不適合報告とツール機能への問題の影響の評価の概要を含む。加えて、ツールの全ての機能的制限を含まなければならない。

(j) 適合性宣言

この項は、この資料への遵守とツール計画で明確にされた条件への遵守の実証に利用される手法の概要の供述を含む。この項は認証機関が作成した追加のルールとツール完了報告のどこにも取り扱われていないツール計画、標準、この資料からの全ての逸脱を扱う。

《10.1.15》

【11】

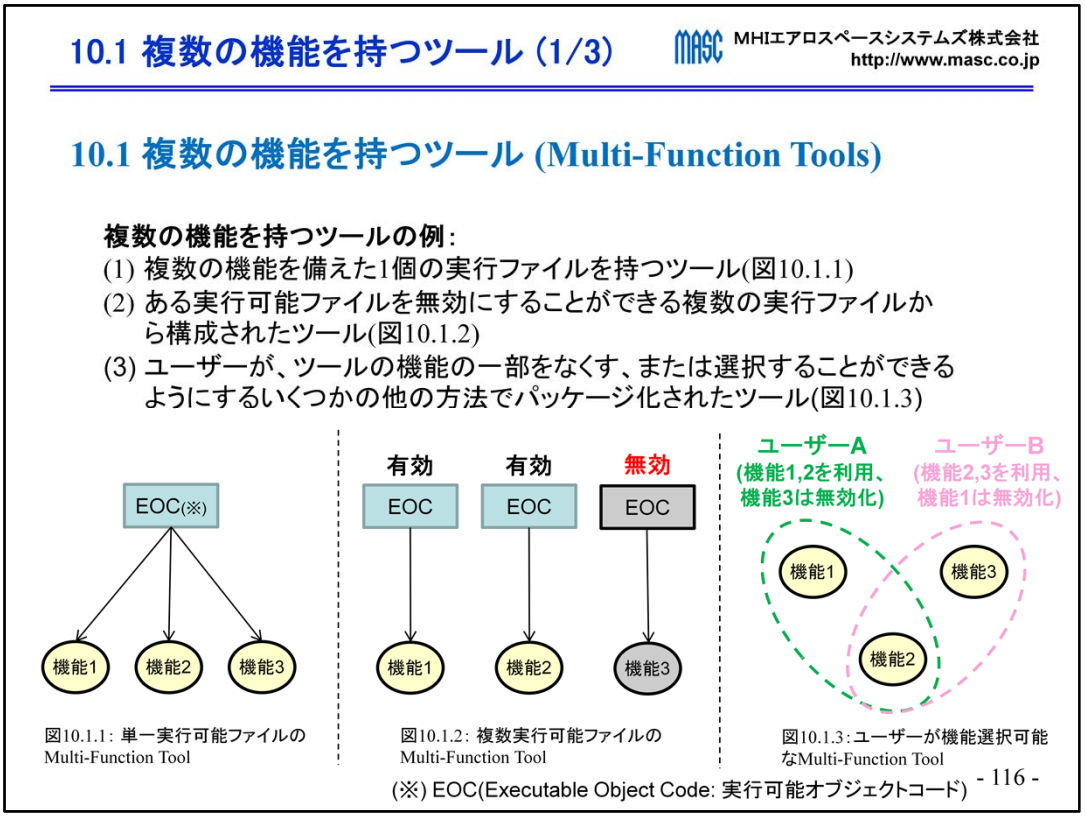
ここでは、11章に記載されている追加の考慮事項(Additional Considerations)について説明する。
11章では、以下の5項目について記載されている。

1. 複数の機能を持つツール (Multi-Function Tools)
2. 既に資格化されたツール (Previously Qualified Tools)
3. COTSツールに資格を与えること (Qualifying COTS Tools)
4. サービス履歴 (Service History)
5. ツール資格化のための代替手法 (Alternative Methods for Tool Qualification)

《11.0》ツール資格のための追加の考慮事項 (Additional Considerations for Tool Qualification)

本資料の前のセクションで記載した目的(Objectives)への準拠を達成するため、このセクションでは、複数の機能を持ったツールの利用、既に資格化されたツール、COTSツール、サービル履歴、そして代替手法に関連して、ツール資格に関する追加の考慮事項についてのガイダンスを提供する。

《11.0》



【11.1】

複数の機能を持つツールを資格化する際のガイダンスを述べている。本文では、複数の機能を持つツールの3つの例をあげている。

1つ目は、「複数の機能を備えた1個の実行可能ファイルを持つツール」である(図10.1.1)。

2つ目は、「ある実行可能ファイルを無効にすることができる複数の実行ファイルから構成されたツール」である(図10.1.2)。

3つ目は、「ユーザーが、ツールの機能の一部をなくす、または選択することができるようにするいくつかの他の方法でパッケージ化されたツール」である。これは起動オプションなどによって、ユーザー毎にツールで利用したい機能を選択できるようなツールであると思われる。

ただしDO-330では複数の機能があるツールであっても、中には使わない機能があっても良いとされている。例えば、開発と検証の両機能を持つツールをあるプロジェクトで利用する場合、開発機能のみを使い、検証機能は使わないという決定はしても良い。

《11.1》複数の機能を持つツール (Multi-Function Tools)

複数の機能を持つツールは、複数の機能を実行するものである。複数の機能を持つツールの種類の例には以下のものがある。

・複数の機能を備えた1個の実行可能ファイルを持つツール
・ある実行可能ファイルを無効にすることができる複数の実行可能ファイルから構成されたツール
・ユーザーが、ツールの機能の一部をなくす、または選択することができるようにするいくつかの他の方法でパッケージ化されたツール

機能のいくつかはソフトウェアライフサイクルプロセスを省略、削減、自動化するために使っても良く、いくつかの機能は定められたプロジェクトであっても使われなくても良い。例えば、ツールは複数の開発及び検証機能を含んで良

い。開発及び検証機能のいくつかは使われても良いし、一方で他の機能は特有のプロジェクトに関して必要とされない。

ドメインに関係したガイダンス(domain-related guidance)に従って、適切なTQLは複数の機能を持つツールの各機能のため決定されなければならない。いくつかの機能のみ資格化する場合、又はいくつかの機能で異なるTQLが適用される場合、以下の追加のガイダンスは適用されなければならない。もしそうしなければ、全てのツールは最も高いTQLで資格化されなければならない。

a. いくつかの機能はより下位のTQLで資格化されても良い。これは、より上位のレベルの機能がより下位のTQLの機能(又は機能のグループ)から保護される場合のみ可能である。申請者は、全体的なツール機能と実装を評価し、各機能(又は機能のグループ)に対して提案されるTQLを識別しなければならない。この評価には、各ツール機能の識別、ツール機能間の関係と相互作用、ツールの運用法(operational usage)、ツール形態(tool configuration(s))、そして資格化するつもりの機能の識別が含まれる。

b. 異なるTQLを持つ機能(又は機能のグループ)の間の保護は確認されなければならない。この保護を許可できるエビデンスは、より下位のTQLで資格化される機能(又は機能グループ)のアウトプットが他の機能のアウトプットに影響しない(つまり、ツールの能力は機能上隔離されている)ことを示すことである。異なるTQLが実装される場合、保護のアプローチは各ツール機能に関して実証されなければならない。

c. 異なるTQLの機能(又は機能のグループ)の間での保護が示される場合、保護された機能は、まるでそれらが別のツールであるかのように資格化されても良い。

d. 複数の機能を持つツールが出力を生成し、この同じ出力を検証する場合、両方の機能に影響を与えるかもしれないエラーを避けるための保護技術を利用してツールの機能が開発されたことを確認されなければならない。ツールによって満足される検証objective(verification objective)が独立性を要求されている場合、出力を検証する機能は、出力を生成する機能から独立していることを示されなければならない。独立性とは通常は、ツール機能間に共通のエラーが存在しないことを保証するため、また検証機能が完全に出力中のいかなるエラーも検出することを検証するため利用される。

e. このガイダンスを適用する場合、ツールのいくつかの機能は資格化されなくても良い。これは通常は、ツールの中のいくつかの機能がソフトウェアライフサイクルプロセスで利用されない、又はツールの出力に対してドメインの関係するガイダンス(domain-related guidance)によって要求たように検証を実証する場合である。資格化される機能は、利用されない機能(又は機能のグループ)に依存しないことを示されなければならない。加えて、利用されない機能は、それらが将来の資格化への取り組みで不注意に資格化されるものと思われないよう、明確に識別されなければならない。

全ての複数の機能を持つツールは、適切なツール計画で記載されなければならない。計画は、ツールの機能、TQLの評価、利用予定の機能と利用予定ではない機能の記述、そしてどのように上記のガイダンスを満足させるのかを説明しなければならない。

注意事項:ツールがTQL-5より高い機能を含まない場合、セクション11.1.dのみ適用する。

《11.1》

10.1 複数の機能を持つツール (2/3)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

10.1 複数の機能を持つツール (Multi-Function Tools) （続き）

それぞれの機能ごとに、適切なTQLを設定しなければならない。
ただし、一部の機能だけを資格化する場合や、機能の中で異なるTQLを設定するものがある場合、以下の追加のガイダンスを適用しなければならない。

a. 機能の中には、より低いTQLで資格化されるものもあっても良い。ただし、高いTQLの機能が、それより低いTQLの機能(又は機能グループ)から保護されなければならない。

b. 異なるTQLを持つ機能間の保護は確認されなければならない。このエビデンスは、下位のTQLの機能の出力が、他の機能の出力に影響しないことを示すことである。

c. 異なるTQLの機能(又は機能グループ)間での保護が示される場合、保護された機能は、別のツールであるかのように資格化されても良い。

- 117 -

【11.1】

複数の機能について、異なるTQLを設定しても良い。
ただし、以下の場合は、追加のガイダンスを適用しなければならない。

(1) 一部の機能だけを資格化する
(2) いくつかの機能で異なるTQLを設定する

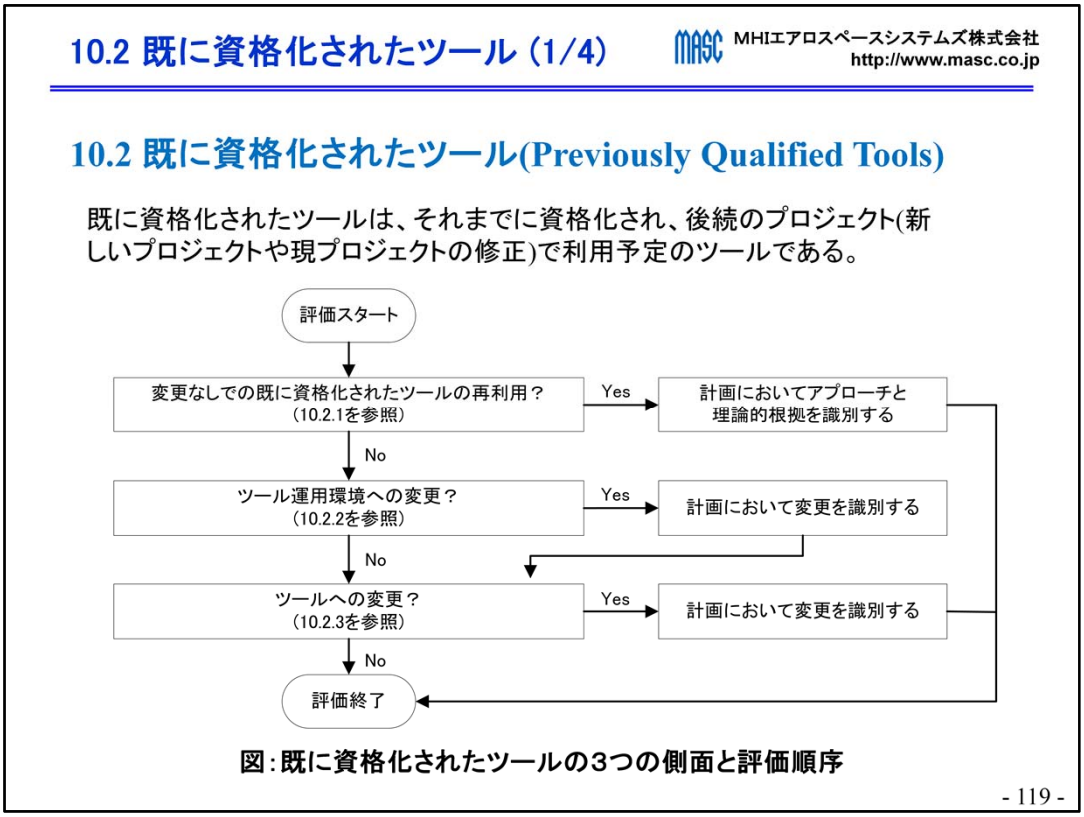
MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

10.1 複数の機能を持つツール (Multi-Function Tools) （続き）

d. 出力を生成し、その出力の検証も行うツールは、両機能に影響を与える可能性のあるエラーを避けるための保護技術が使用され開発されたことを、確認しなければならない。

e. なかには資格化されない機能があっても良い。ただし、資格化される機能は、利用しない機能に依存しないことを示さなければならない。

【11.1】



図：既に資格化されたツールの3つの側面と評価順序

【11.2】

ここでは、既に資格化されたツールの利用について説明する。

既に資格化されたツールには3つの側面があり、次のスライドから各々のガイダンスを提供する。
(1)変更されていない既に資格化されたツールの再利用
(2)ツール運用環境の変更
(3)ツール自体の変更

スライドに示した図は、既に資格化されたツールの3つの側面と評価の順序(order)を表している。

《11.2》既に資格化されたツール (Previously Qualified Tools)

既に資格化されたツール(Previously qualified tools)は、それまでに資格化され、後続のプロジェクト(後続のプロジェクトは新しいプロジェクトや現在のプロジェクトへの修正であっても良い)で利用されるつもりのツールを含む。下記のセクションは、ツール資格の3つの側面についてのガイダンスを提供する。(1) 変更されていない既に資格化されたツールの再利用、(2) ツール運用環境(tool operational environment)への変更、(3)ツールそれ自体への変更、である。図11-1は、既に資格化されたツールの3つの側面と評価の順序(order)を表現している。

《11.2》

10.2 既に資格化されたツール (2/4)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

10.2.1 既に資格化されたツールの再利用
(Reuse of Previously Qualified Tools)

次の基準が満たされる場合、ツールは再利用に適している。

No	基準	Yes	No
1	ツールは、以前のソフトウェアプロジェクトで資格化された。		
2	再利用のためのTQLは、以前の資格より同じか低い。		
3	以前の資格化から、再利用が考えられているツールライフサイクルデータは変更されていない。		
4	ツール運用環境は、以前の資格化のそれと同等であると示される。		
5	ツール運用要求は、以前の資格化の場合と同じである。		
6	申請者は、承認されたツール資格データを利用できる。		
7	申請者は、資格データによって支援されるのと同じツールのバージョンが利用されていることを保証する。		

全ての基準が満たされる場合、ツールデータの再利用のための意図と理論的根拠は、PSACおよび(または)TQPに記載され、認証機関に提出されなければならない。

- 120 -

【11.2.1】

ここでは、過去のプロジェクトで資格化されたツールを、現在のプロジェクトで再利用する場合について述べる。

《11.2.1》既に資格化されたツールの再利用 (Reuse of Previously Qualified Tools)

このセクションは、変更なしで後続のプロジェクトにおいて利用されるだろう以前のプロジェクトで資格化されたツールに関する資格データ(qualification data)の再利用について述べる。

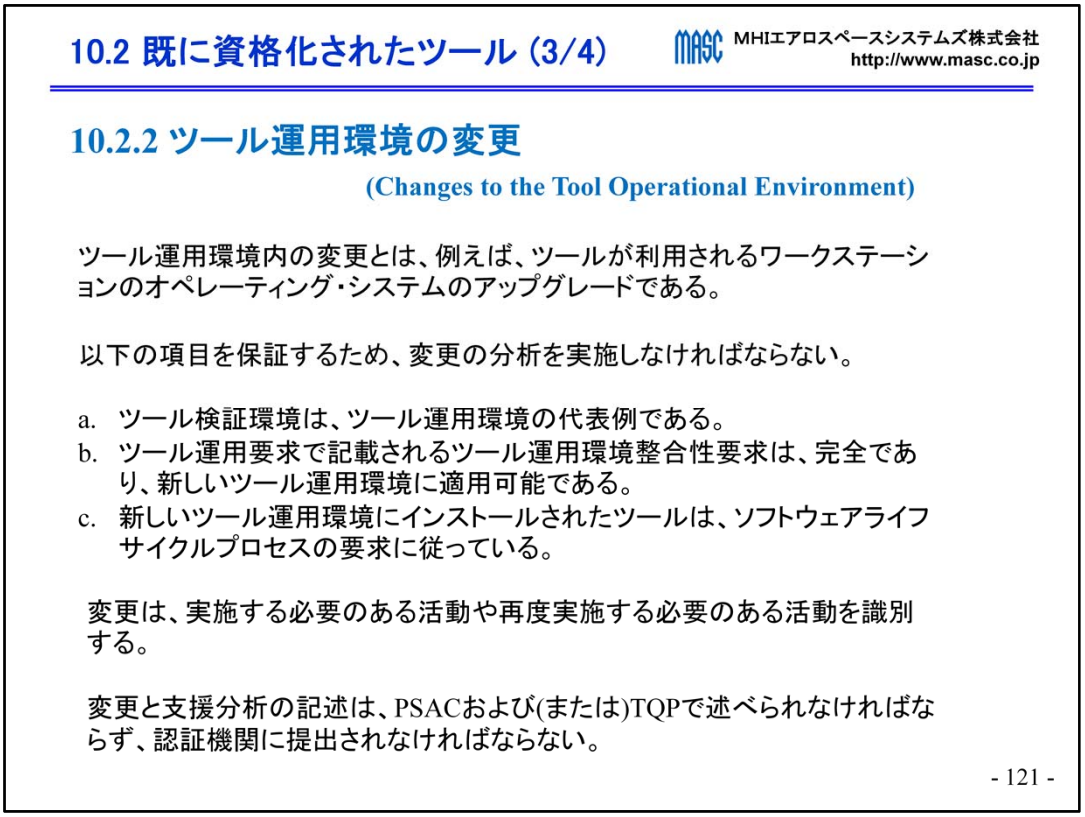
次の基準が満たされる場合、ツールは再利用に適している。

a. ツールは、認証機関によって承認された以前のソフトウェアプロジェクトの範囲内で、既に資格化された。
b. 再利用のためのTQLは、以前の資格より同じ又は低い。
c. ツールの以前の資格化以来、再利用について考慮されているツールライフサイクルデータは変更されていない。
d. ツール運用環境は、以前の資格化のそれと同等であると示される。
e. ツール運用要求(Tool Operational Requirements)は、以前の資格化に関するかぎりでは同様である。
f. 申請者は承認されたツール資格データ(approved tool qualification data)を利用できる。
g. 申請者は、資格データによって支援されるのと同じツールのバージョンが利用されていることを保証する。

基準のいずれかが満たされない場合、セクション11.2.2及び(又は)11.2.3は変更のため解析されなければならない。

もし全ての基準が満たされるのなら、ツールデータの再利用のための意図と理論的根拠はPSAC及び(又は)TQPに記載され、認証機関へ提出されなければならない。さらに、以前に資格化されて以来以前として未解決又は生じている(たとえその後にクローズした場合でも)ツール不適合報告は、評価され、適切に処置されなければならない。

《11.2.1》



【11.2.2】

ツール運用環境の変更とは、例えば、Windows XPからWindows 7へのアップグレードである。

《11.2.2》ツール運用環境への変更(Changes to the Tool Operational Environment)

このセクションはツール運用環境の変更について述べる。例は、ツールが利用されるワークステーションのオペレーティング・システムのアップグレードである。

変更の分析は以下の項目を保証するために行われなければならない。

a. ツール検証環境は、ツール運用環境の代表例(representative)である(4.4.cを参照)。

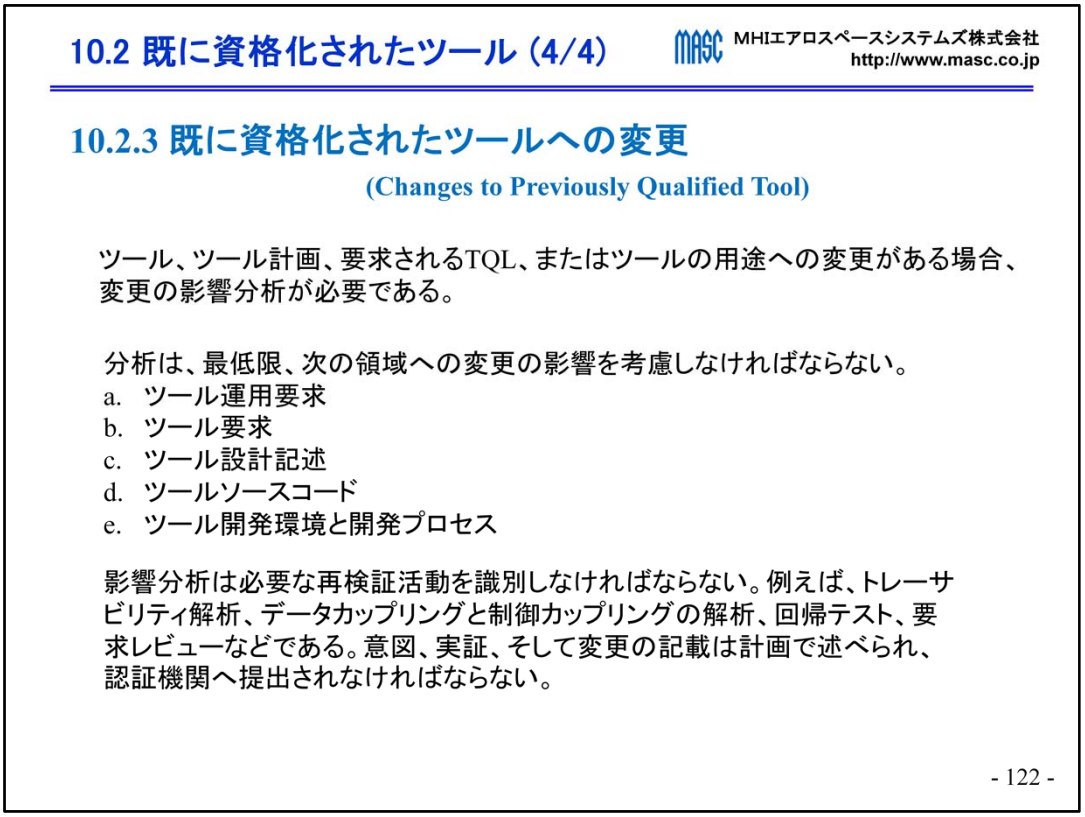
b. ツール運用要求(Tool Operational Requirements)で記載されるツール運用環境互換性要求(tool operational environment compatibility requirements)は、完全であり、新しいツール運用環境に適用可能である(6.2.2.a.2を参照)。

c. 新しいツール運用環境にインストールされたツールは、ソフトウェアライフサイクルプロセスの要求に従っている(6.2.2.cを参照)。

分析は、実施する必要のある活動(activity)や再度実施する必要のある活動を識別する。

以前に資格化されて以来の変更と支援解析の記載は、PSAC及び/又はTQP内で述べられなければならず、認証機関に提出されなければならない。

《11.2.2》



【11.2.3】

《11.2.3》既に資格化されたツールへの変更 (Changes to Previously Qualified Tool)

このセクションは、後続のプロジェクトにおける既に資格化されたツールへの変更について述べる。

ツール、ツール計画、要求されるTQL、またはツールの用途への変更がある場合、変更影響分析(change impact review)が必要である。分析は、最低限、次の領域への変更の影響を考慮しなければならない。

a. ツール運用要求(Tool Operational Requirements)
b. ツール要求(Tool Requirements)
c. ツール設計記述(Tool Design Description)
d. ツールソースコード(Tool Source Code)
e. ツール開発環境と開発プロセス

この影響分析(impact analysis)は必要な再検証活動を識別しなければならない。例えば、トレーサビリティ解析、データカップリングとコントロールカップリングの解析、回帰テスト(regression testing)、要求レビュー(requirements review)等である。

変更の意図、実証(substantiation)、そして記載は計画で述べられ、認証機関へ提出されなければならない。

《11.2.3》

10.3 COTSツールに資格を与えること (Qualifying COTS Tools)

COTSツールは、特有のソフトウェアプロジェクトから独立して開発され、多数のユーザーに利用される。

COTSツールは、他のツールと同様に、適切なTQLを設定し、資格化のための目的(objective)を満足しなければならない。しかし、異なるプロセスを実行するツールのユーザーと開発者の間の責任の分離が、提案されなければならない。

【11.3】

ここではCOTSツールを資格化する場合について述べる。

COTSツールを利用する際は、ユーザーと開発者などの関係者を定義し、それらの間で補足的にプロセスを実行していかなければならない。

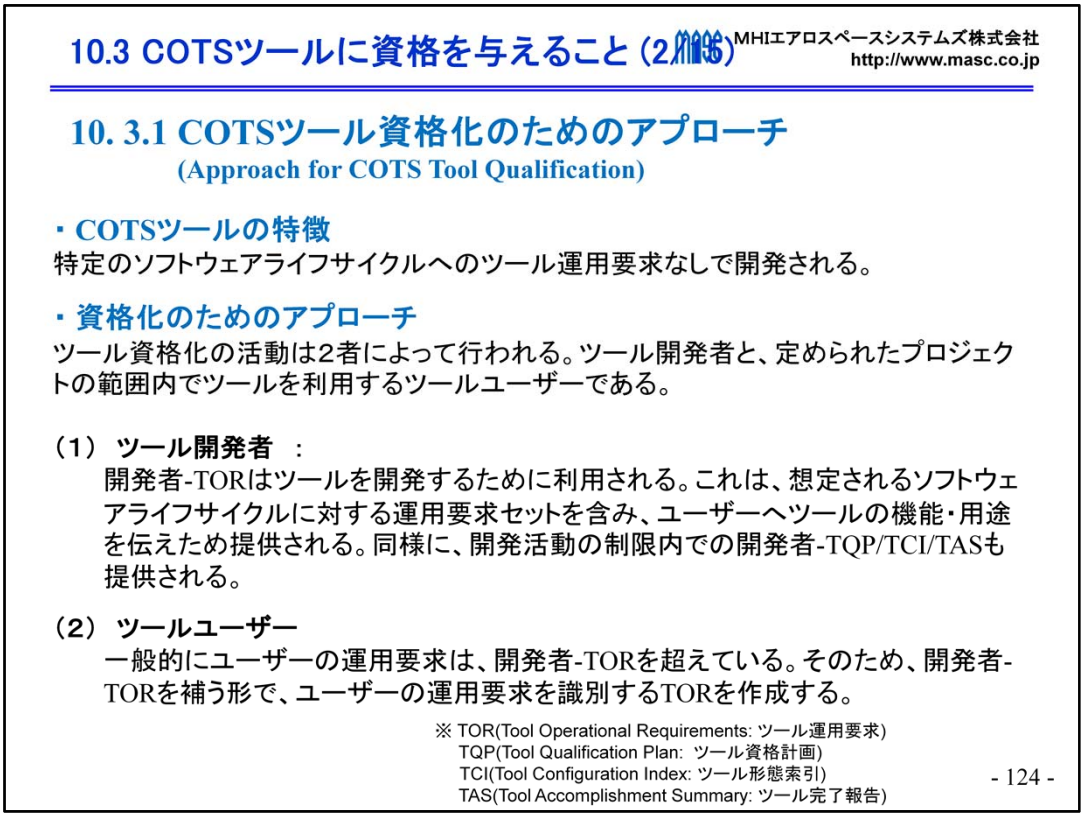
《11.3》COTSツールに資格を与えること (Qualifying COTS Tools)

このセクションは、COTSツール適用に対して本資料のツール資格のガイダンスを適合(adapt)させる。一般的にCOTSツールは、特有のソフトウェアプロジェクトから独立して開発され、多数のユーザーに利用されることを意図されている。

ユーザーマニュアルで記載されるようにツールユーザーによって設定可能であるよう設計されたCOTSツールは、このセクションのガイダンスの下で網羅(cover)される。ツールユーザーによって改変されるツールは対象外である。

COTSツールは、資格化される他のツールのように、必要なTQLに適切な目的(Objectives)に準拠する必要がある。しかしながら、異なるプロセス(ツール運用開発プロセス、ツール開発プロセス、そして全ての関連する検証プロセス)の目的(objective)を満たすため、ツールユーザーとツール開発者の間の責任の分離が提案されなければならない。

《11.3》



【11.3.1】

COTSツールは、特定のソフトウェアライフサイクルへのツール運用要求なしで開発される。

つまり、ツールユーザーによって作成されたツール運用要求(Tool Operational Requirements)からツールが作られるわけではない。

《11.3.1》COTSツール資格化のためのアプローチ (Approach for COTS Tool Qualification)

一般的にCOTSツールは、特有のソフトウェアライフサイクルに利用できるツール運用要求(Tool Operational Requirements)なしで開発される。ユーザーへツールの機能と用途を伝えるため、ツール開発者は、考えられるソフトウェアライフサイクルに対する運用要求のセットを含む開発者-TORを提供しなければならない。ツールユーザーは、ツールがソフトウェアライフサイクルの要求を満たすかどうかを決定するため開発者-TORを使うだろう。ツールユーザーは、ツールの運用上の利用のための要求を識別しているTORを提供する。典型的にTORは、開発者-TORを超えている。

COTSツールのため、典型的にツール資格化の活動(tool qualification activities)は以下の2者によって行われる。

ツール開発者:ツールを開発する者

ツールユーザー:定められたソフトウェアプロジェクトの範囲内でツールを利用する者

全てのツール資格化の目的を満たすため、活動はCOTSツール開発者とツールユーザーの両方のため以下に定義される。TQL-5資格化のため、目的(objectives)はツール開発者からのツール資格データなしで満たされても良いことに注意しなければならない。

《11.3.1》

10.3 COTSツールに資格を与えること (3/16)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

10. 3.2 ツール開発者のための活動

(Activities for the Tool Developer)

資格化できるツールを提供するため、
ツール開発者は以下の項目を行わなければならない。

a. ツール開発者へ割当てられた全ての目的(objectives)が満たされたことを確認するため、本資料のガイダンスを使用しなければならない。表10.3.1に、ツールのユーザー / 開発者に一般的に適用される目的(Objectives)をまとめた。

b. ツールに実装された機能を識別するため開発者-TORを提供しなければならない。

c. TQLに適した予備的なツール資格データの適切なセットを提供しなければならない。

- 125 -

【11.3.2】

《11.3.2》ツール開発者のための活動 (Activities for the Tool Developer)

資格化できるツールを提供するため、ツール開発者は以下の項目をしなければならない。

・ツール開発者へ割当てられた全ての目的(Objectives)が満たされたことを確認するために必要とする活動を実行し、またツールライフサイクルデータを作成するために、本書のガイダンスを使用しなければならない。

・ツールに実装された機能を識別するため開発者-TORを提供しなければならない(11.3.2.1を参照)

・TQLに適した予備的なツール資格データのセットを提供しなければならない(11.3.2.2から11.3.2.4)

表11-1は、ツール開発者に一般的に適用される目的(Objectives)を識別する。

《11.3.2》

10.3 COTSツールに資格を与えること (4/16)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

10. 3.2.1 開発者-TOR (Developer-TOR)

ツールが、ユーザーの要望を満たすかどうかをツールユーザー決定できるように、開発者-TORは開発されなければならない。修正なしでツールユーザーがTORから直接参照しても良いデータでなければならない。

開発者-TORには下記項目が記載されなければならない。

a. 予期される全てのツール運用環境の記述
b. フォーマット、言語の定義など、入力ファイルの記述
c. フォーマットとコンテンツなど、出力ファイルの記述
d. ツールの期待される全ての機能の振る舞いのための要求(ソフトウェアライフサイクルプロセスの観点から)
e. ツールによって検出されなければならない異常活動モードや矛盾した入力を述べるための要求。これらの要求は、機能のそれらのモードとツールの出力の影響を考慮しなければならない。
f. ユーザーマニュアルやインストールガイド (または、ツール要求データの一部として提供されない場合には、それへのリファレンス) のような、利用できるユーザー情報

- 126 -

【11.3.2】

《11.3.2.1》開発者-TOR (Developer-TOR)

ツールがユーザーの要望を満たすかどうかをツールユーザー決定できるように、開発者-TORは開発されなければならない。開発者-TORは、修正なしでツールユーザーがTORから直接参照しても良いデータを含まなければならない。

本資料で記載されるTORの代わりに、開発者-TORはツール開発者によって使われる。

開発者-TORは下記項目を含まなければならない。

a. 予期される全てのツール運用環境(tool operational environments)の記述

b. フォーマット、言語の定義など、入力ファイルの記述(10.3.1.cを参照)

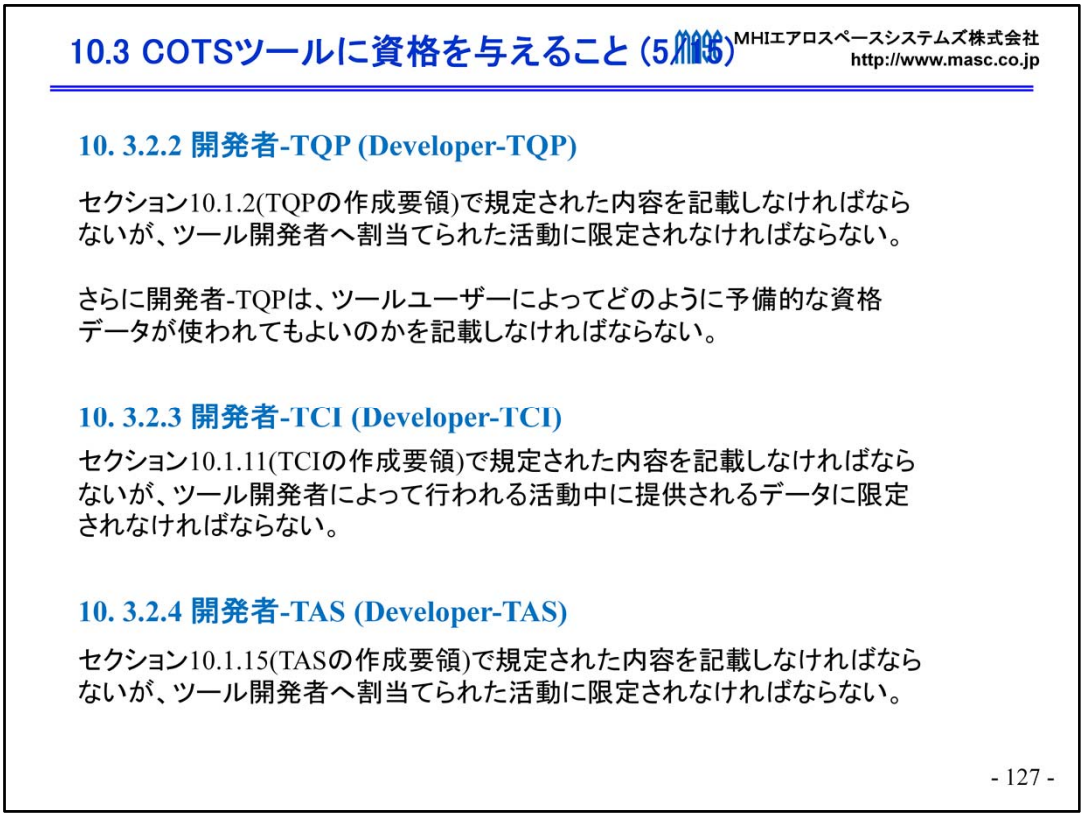
c. フォーマットとコンテンツなど、出力ファイルの記述(10.3.1.dを参照)

d. ツールの期待される全ての機能の振る舞いのための要求(ソフトウェアライフサイクルプロセスの観点から)(10.3.1を参照)

e. ツールによって検出されなければならない異常活動モード(abnormal activation modes)や矛盾した入力(inconsistency inputs)を述べるための要求。これらの要求は、機能性におけるそれらのモードとツールの出力の影響を考慮しなければならない。(10.3.1.fを参照)

f. ユーザーマニュアルやインストールガイド (または、ツール要求データ(Tool Requirements data)の一部として提供されない場合には、それへのリファレンス) のような、利用できるユーザー情報(10.3.1.g)を参照

《11.3.2.1》



10.3 COTSツールに資格を与えること (5/MASC)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

10. 3.2.2 開発者-TQP (Developer-TQP)

セクション10.1.2(TQPの作成要領)で規定された内容を記載しなければならないが、ツール開発者へ割当てられた活動に限定されなければならない。

さらに開発者-TQPは、ツールユーザーによってどのように予備的な資格データが使われてもよいのかを記載しなければならない。

10. 3.2.3 開発者-TCI (Developer-TCI)

セクション10.1.11(TCIの作成要領)で規定された内容を記載しなければならないが、ツール開発者によって行われる活動中に提供されるデータに限定されなければならない。

10. 3.2.4 開発者-TAS (Developer-TAS)

セクション10.1.15(TASの作成要領)で規定された内容を記載しなければならないが、ツール開発者へ割当てられた活動に限定されなければならない。

- 127 -

【11.3.2】

《11.3.2.2》開発者-TQP (Developer-TQP)

開発者-TQPは、セクション10.1.2で特定されるのと同じコンテンツを持たなければならないが、ツール開発者へ割当てられたそれらの活動へ限定されなければならない。さらに開発者-TQPは、ツールユーザーによってどのように予備的な資格データ(preliminary qualification data)が使われてもよいのかを記載しなければならない。

《11.3.2.2》

《11.3.2.3》開発者-TCI (Developer-TCI)

開発者TCIは、セクション10.1.11で特定されるのと同じコンテンツを持たなければならないが、ツール開発者によって行われる活動の間に提供されるデータへ限定されなければならない。

《11.3.2.3》

《11.3.2.4》開発者-TAS (Developer-TAS)

開発者-TASは、セクション10.1.15で特定されるのと同じコンテンツを持たなければならないが、ツール開発者へ割当てられたそれらの活動へ限定されなければならない。

《11.3.2.4》

10.3 COTSツールに資格を与えること (6/11)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

10. 3.3 ツールユーザーのためのツール資格化の活動
(Tool Qualification Activities for the Tool User)

・ツールの選定・評価

ソフトウェア計画プロセスの間にCOTSツールの選定を行うため、
COTSツールに対して以下を評価しなければならない。

(1) 提案されたソフトウェアライフサイクルプロセスとの整合性
(2) ツール運用環境との整合性
(3) COTSツールのライフサイクルデータと予備的な資格データの可用性(availability)と妥当性(relevance)

・ツール開発者のデータ・活動の補完

(1) 目的(Objectives)全てを満足させるのに不十分な開発者データの場合、ユーザーはデータを補わなければならない。
(2) ツール運用環境でCOTSツールを評価するため、ツールユーザーは開発者の活動を補わなければならない。表10.3.1に、ツールのユーザー / 開発者に一般的に適用される目的(Objectives)をまとめた。

- 128 -

【11.3.3】

《11.3.3》ツールユーザーのためのツール資格化の活動 (Tool Qualification Activities for the Tool User)

COTSツールの選定は、一般的にソフトウェア計画プロセスの間に行われる。このプロセスの間、ユーザーは提案されたソフトウェアライフサイクルプロセスの要求及びそのツール運用環境との整合性を満たす能力についてCOTSツールを評価しなければならない。適切なTQLの資格化を支援するためCOTSツールライフサイクルデータと予備的な資格データのセット(preliminary set of qualification data)の可用性(availability)と妥当性(relevance)もまた、ソフトウェアプロジェクト内のコンテキストで評価されなければならない。

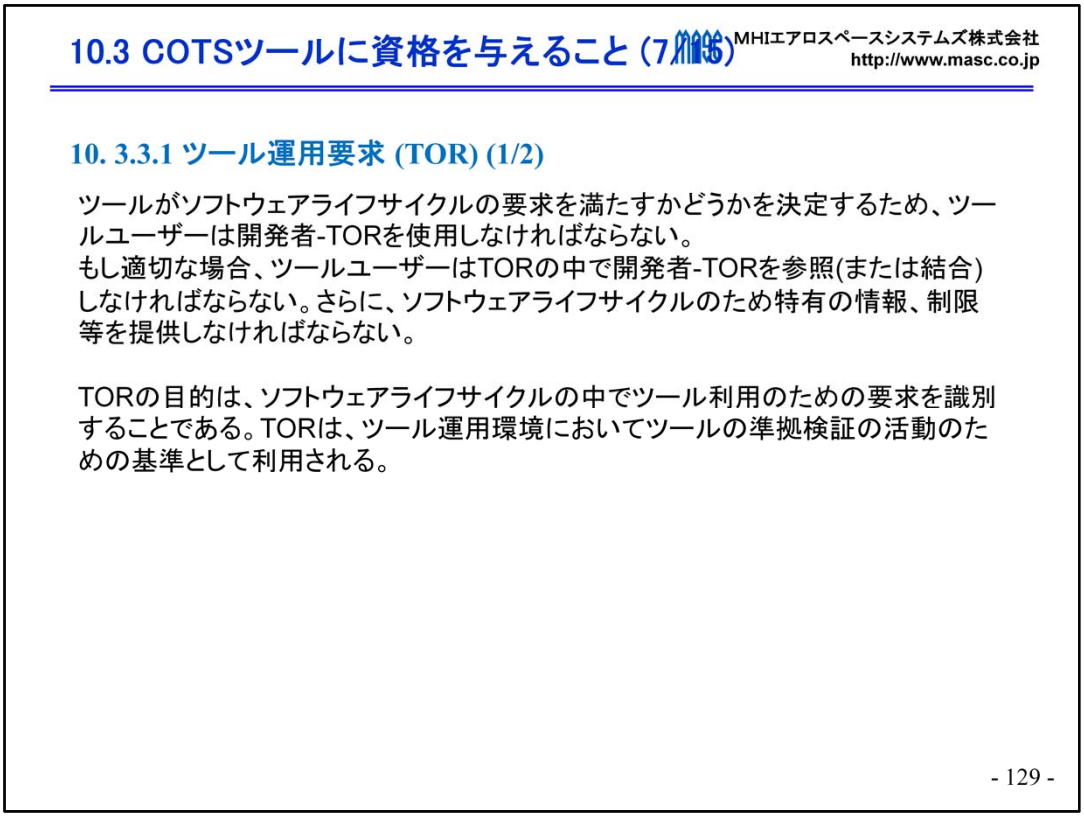
既に資格化されたCOTSツールは、承認を要求される他のプロジェクトのため資格化されると自動的にはみなされない。(既に資格化されたツールのガイダンスについては11.2を参照)

もし現存するツールライフサイクルデータが、ツール開発者に適用される目的(Objectives)の全てに適合することを確認するのに十分でないなら、ツールユーザーはデータを増やさなければならず、そして(又は)代替手法を提案しなければならない(11.5を参照)。このアプローチはTQPに記載されなければならない。

ツール運用環境でCOTSツールを評価するため、ツールユーザーは開発者の活動を補わなければならない。表11-2に、ツールユーザーに一般的に適用される目的(Objectives)を識別する。

TOR, TQP, TCI,そしてTASのため、ツールユーザーはセクション11.3.3.1から11.3.3.4の推奨事項を考慮しなければならない。

《11.3.3》



【11.3.3】

《11.3.3.1》ツール運用要求(TOR) (Tool Operational Requirements(TOR))

ツールユーザーは、ツールがソフトウェアライフサイクルの要求を満たすかどうかを決定するため開発者-TORを利用しなければならない。もし適切な場合、ツールユーザーはTORの中で開発者-TORを参照または結合(incorporate)させなければならず、そしてソフトウェアライフサイクルのため特有の情報、制限等を提供しなければならない。

TORの目的は、ソフトウェアライフサイクルの中でツール利用のための要求を識別することである。TORは、ツール運用環境(tool operational environment)においてツールの準拠検証の活動のための基準として利用される。

TORは以下の項目を含めるべきであるが、限定されるものではない。

a. 開発者TORコンテンツまたは適用可能な開発者-TORコンテンツへの参照
b. 他のツールとのインターフェース、結果としてできるソフトウェアの中のツール出力ファイルの統合など、ツール利用のコンテキスト(context)の記述
c. (ツールがインストールされるだろう)ツール運用環境の記述。これは、開発者-TORに含まれる予想されるツール運用環境の分析を含む(10.3.1.bを参照)。
d. ツールの運用上の利用(選択オプション、パラメータ値、コマンドライン等)の記述(10.3.1.hを参照)
e. 特定された運用環境でのツールの運用入力(operational inputs)の記述。この記述の目的は、考えられる全ての入力データとそれに関連する構造(its associated structure)を識別することである。この記述の完全性(completeness)と正確性(accuracy)は、ツールの運用上の利用を含むツール運用検証データの開発を許すだろう。(10.3.1.cを参照)
f. ツール出力の振る舞いを特定する性能要求(10.3.1.iを参照)

《11.3.3.1》

10.3 COTSツールに資格を与えること (8/11)

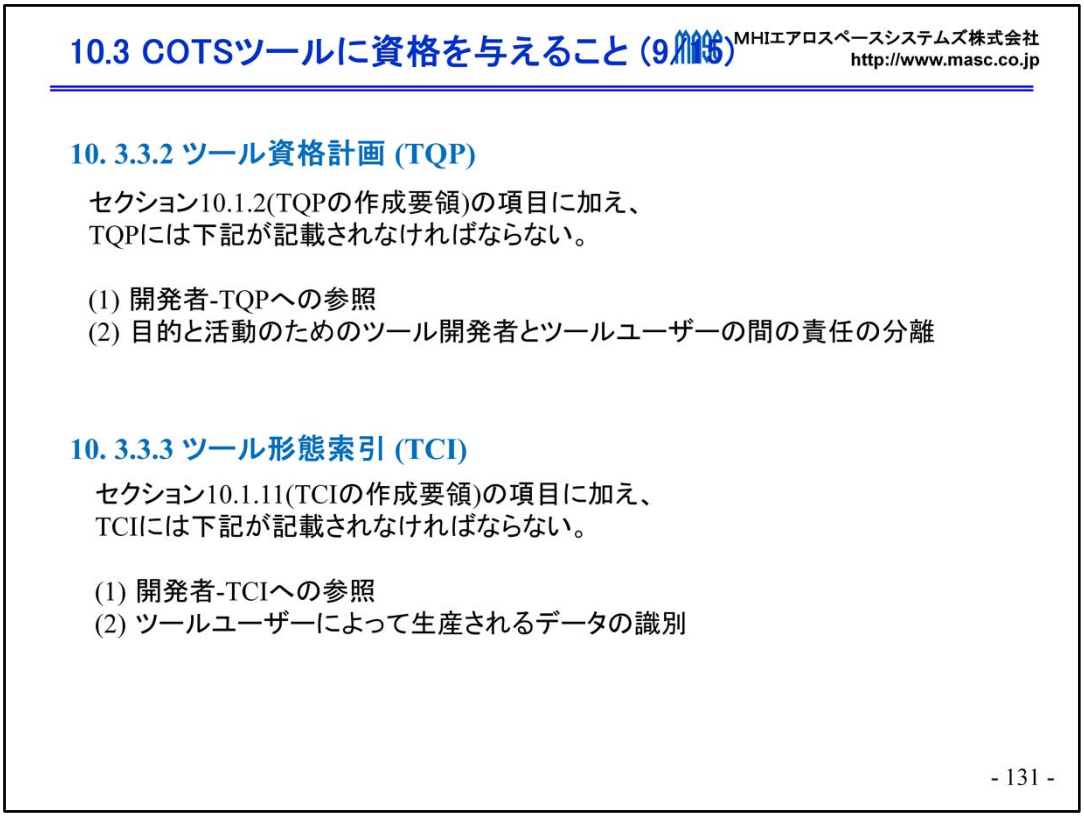
MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

10. 3.3.1 ツール運用要求 (TOR) (2/2)

TORは以下の項目を含めるべきであるが、限定されるものではない。

a. 開発者-TORまたは適用される開発者-TORへの参照
b. ツール利用のコンテキストの記述
c. ツール運用環境の記述。これは、開発者-TORに含まれる予想されるツール運用環境の分析を含む(10.3.1.bを参照)。
d. ツール運用上の利用(選択オプション、パラメータ値、コマンドライン等)の記述(10.3.1.hを参照)
e. 特定された運用環境でのツールの運用入力の記述。この記述の目的は、考えられる全ての入力データとそれに関連する構造を識別することである。
f. ツール出力の振る舞いを特定する性能要求(10.3.1.iを参照)

【11.3.3】



【11.3.3】

《11.3.3.2》ツール資格計画(TQP) (Tool Qualification Plan (TQP))

セクション10.1.2で提供される情報に加え、TQPは下記項目を提供しなければならない。

a. 開発者-TQPへの参照
b. 目的(objectives)と活動のためのツール開発者とツールユーザーの間の責任の分割

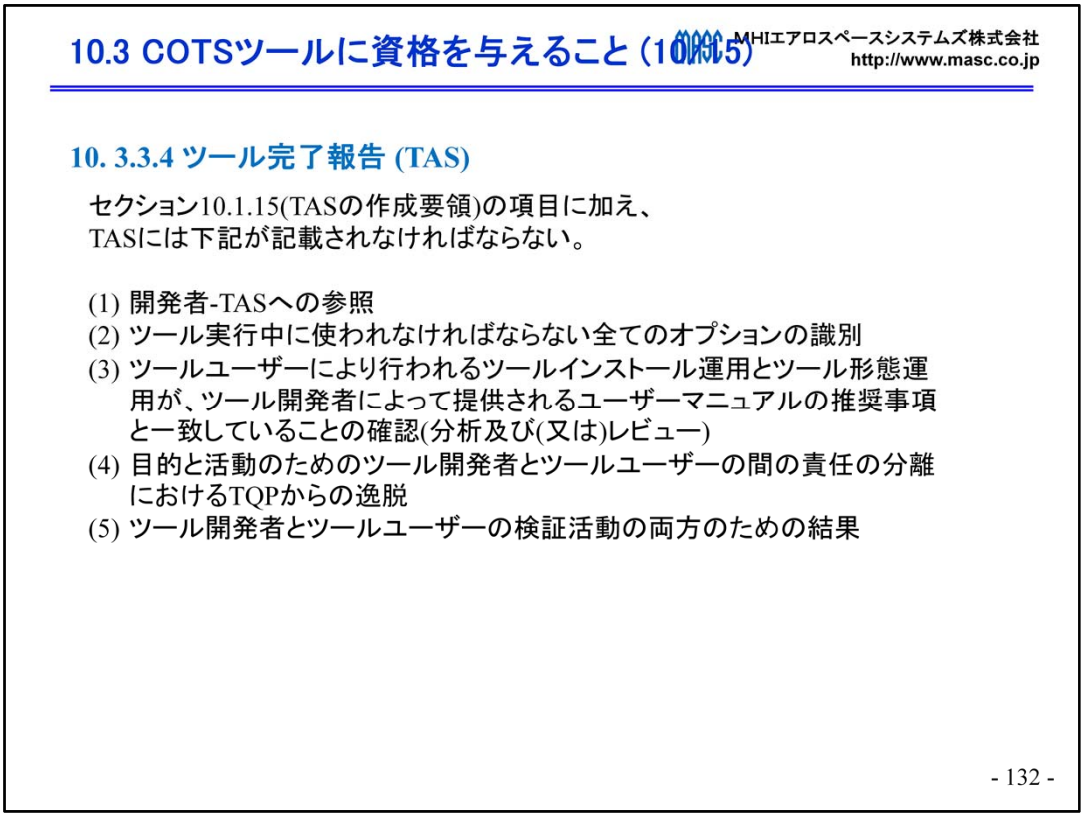
《11.3.3.2》

《11.3.3.3》ツール形態索引(TCI) (Tool Configuration Index (TCI))

セクション10.1.11で提供される情報に加え、TCIは下記項目を提供しなければならない。

a. 開発者-TCIへの参照
b. ツールユーザーによって生産されるデータの識別

《11.3.3.3》



【11.3.3】

《11.3.3.4》ツール完了報告 (TAS) (Tool Accomplishment Summary(TAS))

セクション10.1.15で提供される情報に加え、TASは下記項目を提供しなければならない。

a. 開発者-TASへの参照

b. ツールの実行の間に使われなければならない全てのオプションの識別

c. ツールユーザーによって行われたツールインストールの操作(tool installation operation)とツール形態の操作(tool configuration operation)が、ツール開発者によって提供されるユーザーマニュアルの推奨事項と一致していることの確認(分析及び(又は)レビュー)

d. 目的(Objectives)と活動のためのツール開発者とツールユーザーの間の責任の分割(division)におけるTQPからの逸脱

e. ツール開発者とツールユーザー両者の検証活動の結果

ツールユーザーは、認証機関に提供する全ての資格データを作らなければならない。一般的にツールユーザーは、最後のツール資格ライフサイクルデータの中でツール開発者によって提供された予備的なデータを統合又は参照するだろう。

《11.3.3.4》

10.3 COTSツールに資格を与えること (1 of 5)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

表13.3.1: 一般的なツールのユーザー/開発者のObjectivesの分離 (1/3)

No	目的(Objectives)	担当者	Notes
	Table T-0：ツール運用プロセス		
	計画プロセス		
1	ツール資格の必要性が確立されている	ユーザー	
	ツール運用要求プロセス		
2	ツール運用要求(TOR)は定義されている	両者	開発者：開発者-TORを提供する。 ユーザー：開発者によって提供された開発者-TORを補うTORを作成する。
	ツール運用統合プロセス		
3	ツール実行可能オブジェクトコードは、ツール運用環境にインストールされている。	ユーザー	
	ツール運用検証/妥当性確認プロセス		
4	ツール運用要求(TOR)は完全であり、正確であり、検証可能であり、一貫している。	開発者	開発者-TORを使って行われる。
5	ツール運用はツール運用要求(TOR)に準拠している	開発者	開発者-TORを使って行われる。
6	ツール運用要求(TOR)は十分であり、正しい。	ユーザー	TORがユーザーの運用要求を満たすことを評価するため、TORを検証する。
7	ツールによって、ソフトウェアライフサイクルプロセスの要求が満たされている	ユーザー	TORを利用して行う

- 133 -

この表は、原文の表11-1及び表11-2を一つにまとめたものであり、COTSツールを利用する際の一般的なツール開発者とツールユーザーの満たすべきObjectivesを示している。例えば、Table T-0.1のobjectiveである「ツール資格の必要性が確立されている」は、ユーザー側が満足すべきObjectivesである。

10.3 COTSツールに資格を与えること (12/15)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

表13.3.1: 一般的なツールのユーザー/開発者のObjectivesの分離 (2/3)

No	目的(Objectives)	担当者	Notes
Table T-1: ツール計画プロセス			
1	ツール開発プロセス、インテグラルプロセスが定義されている	両者	目的(Objective)の範囲は、それぞれの特有の活動に制限される。
2	ツールプロセス間の移行基準、相互関係、シーケンス処理が定義されている。	両者	目的(Objective)の範囲は、それぞれの特有の活動に制限される。
3	ツール開発環境が選択され、定義されている。	開発者	
4	追加の考慮事項が示されている	両者	目的(Objective)の範囲は、それぞれの特有の活動に制限される。
5	ツール開発標準が定義されている	開発者	
6	ツール計画がDO-330に準拠している	両者	目的(Objective)の範囲は、それぞれの特有の活動に制限される。
7	ツール計画の開発と改訂が調整されている。	両者	目的(Objective)の範囲は、それぞれの特有の活動に制限される。

- 134 -

Table T-1の1, 2, 4, 6, 7は両者(ユーザーと開発者)によって満たされる目的であり、それぞれ特有の活動に制限される。これらにおいて、特にユーザーは、開発者によって開発されたデータを補うことになる。また、開発者とユーザーの活動間の調整は計画されなければならない。

Table T-1の3と5は、開発者に完全に適用できる目的である。

10.3 COTSツールに資格を与えること (13/15)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

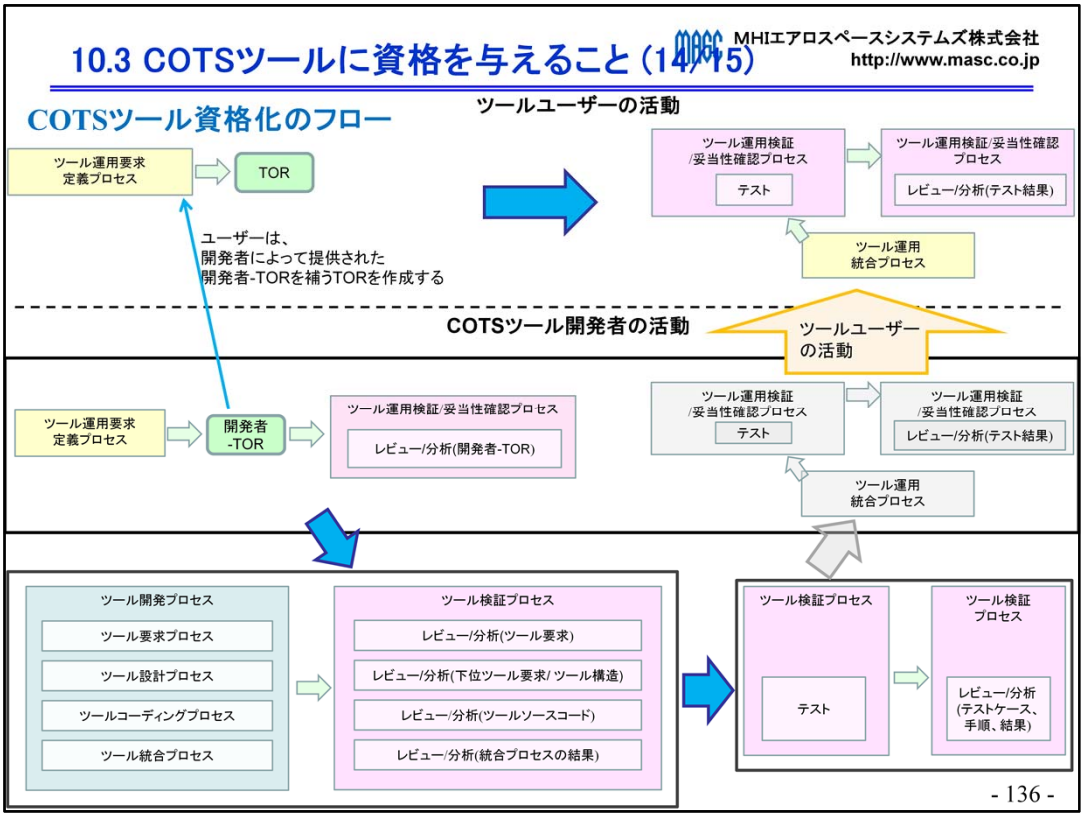
表13.3.1: 一般的なツールのユーザー/開発者のObjectivesの分離 (3/3)

No	目的(Objectives)	担当者	Notes
Table T-2: ツール開発プロセス			
全て		開発者	
Table T-3, T-4, T-5, T-6, T-7: ツール検証プロセス			
全て		開発者	
Table T-8: ツール形態管理プロセス			
全て		両者	目的(Objective)の範囲は、それぞれの特有の活動に制限される。
Table T-9: ツール品質保証システム			
全て		両者	目的(Objective)の範囲は、それぞれの特有の活動に制限される。
Table T-10: ツール認証連絡プロセス			
全て		ユーザー	

- 135 -

ツール開発プロセスとツール検証プロセスの目的は、全てツール開発者に適用される。

ツール認証連絡プロセスの目的は、全てツールユーザーに適用される。



COTSツールを資格化するときの、ツール開発ライフサイクル、ツール開発プロセス、テストプロセスの一般的なフローを図に示す。
上側がツールユーザーの活動、下側がCOTSツール開発者の活動である。

ツール開発者は、開発者-TORを作成して、ツールを作成する。
そして、ツールユーザに各種データを提供する。

ツールユーザーは、ツール開発者から提供された開発者-TORを補いTORを作成する。
ツールの運用統合プロセスは、TORを利用してツールユーザーが行う。

10. 3.4 開発者とユーザーの活動の調整
(Coordination of Developer and User Activities)

最終的にはツールユーザーが資格化のための責任を負う。そのため、ツール開発者により満たされる目的は、ツールユーザーにより評価されるであろう。

TQPは開発者-TQPを参照しなければならず、調整のための手段を提供しなければならない。開発者-TASと開発者-TCIを参照するTASとTCIも同様である。

ツール適合レビューの間、ツールユーザーはツール開発者の適合レビュー報告を分析しなければならず、必要であれば、このレビューの間に発生した是正処置のステータスを検証しなければならない。

【11.3.4】

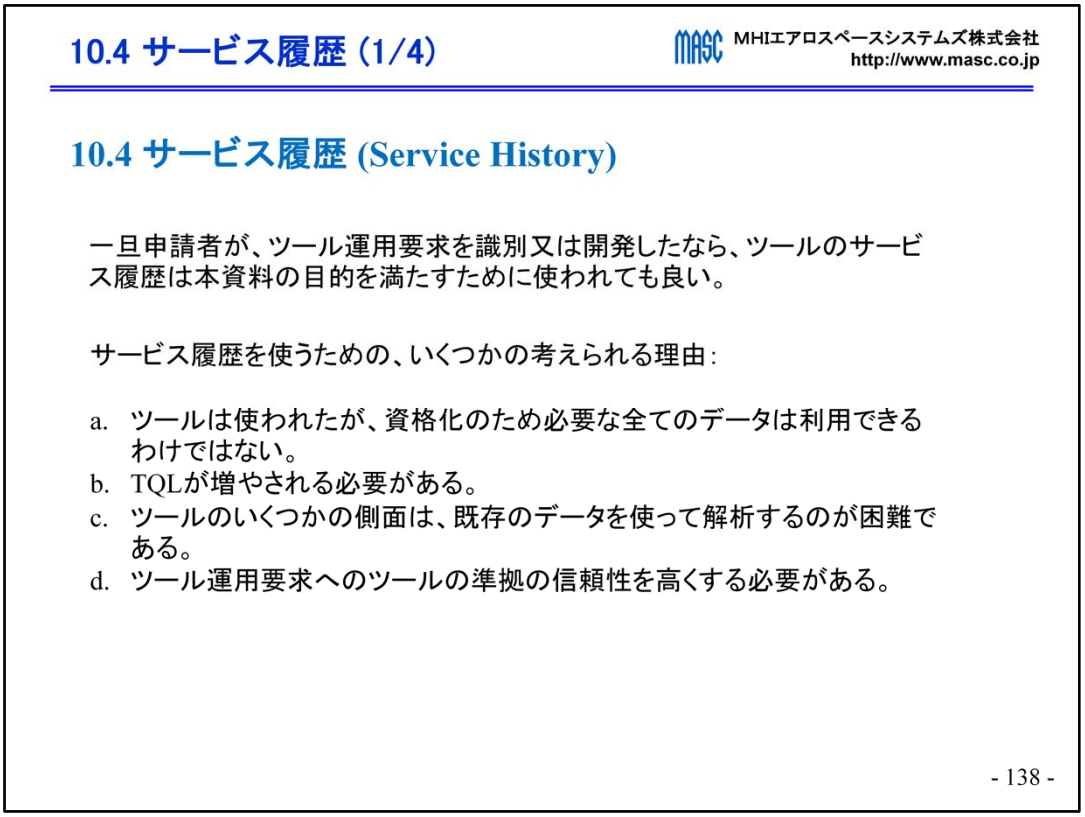
《11.3.4》開発者とユーザーの活動の調整 (Coordination of Developer and User Activities)

最後にはツールユーザーが資格化のための責任を負うので、ツール開発者によって行われる目的(Objectives)はツールユーザーによって評価されるだろう。

TQPは開発者-TQPを参照しなければならず、調整のための手段を提供しなければならない。開発者-TASと開発者-TCIを参照するTASとTCIも同様である。

ツール適合レビューの間、ツールユーザーはツール開発者の適合レビュー報告を分析しなければならず、必要であれば、このレビューの間に発生した是正処置(corrective actions)のステータスを検証しなければならない。

《11.3.4》



【11.4】

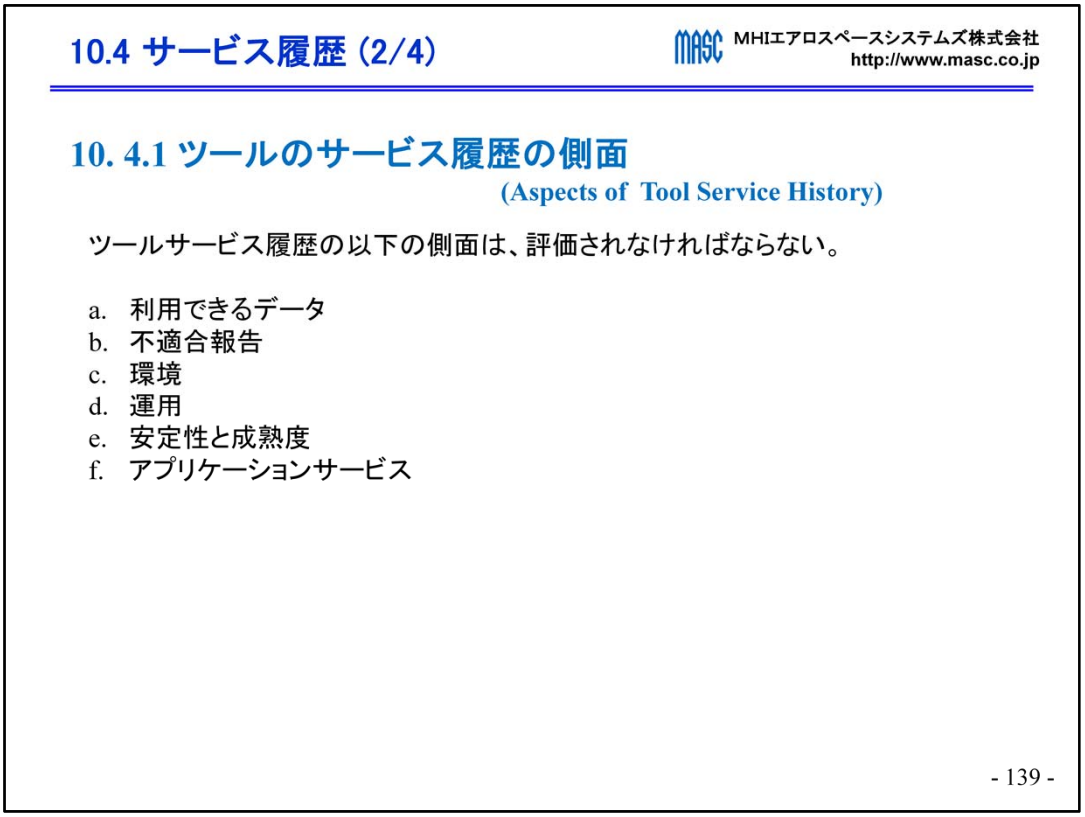
《11.4》サービス履歴 (Service History)

一度申請者が、ツール運用要求(Tool Operational Requirements)を識別又は開発したなら、ツールのサービス履歴は本資料の目的(objectives)を満たすために使われても良い。サービス履歴が使われる場合、その妥当性(relevance)は実証されなければならない。サービス履歴は一件ごとに評価される。

サービス履歴を使うための、いつくかの考えられる理由は以下である。

a. ツールは使われたが、資格化のため必要な全てのデータを利用できない。
b. TQLが増やされる必要がある。
c. ツールのいくつかの側面は、既存のデータを用いて解析するのが困難である。
d. ツール運用要求(Tool Operational Requirements)へのツール準拠の信頼性(confidence)は、高くする必要がある。

《11.4》



【11.4.1】

《11.4.1》ツールのサービス履歴の側面 (Aspects of Tool Service History)

ツールサービス履歴の以下の側面は評価されなければならない。

a. 利用できるデータ(Available data): 利用できるツールサービス履歴データと、ツール運用要求(Tool Operational Requirements)への準拠の証明のその(its)妥当性を識別する。

b. 不適合報告(Problem reporting): 不適合報告とTCMは、最低限、サービス履歴を支援する必要がある。不適合報告は、問題の一貫した定義、問題の分類(classification)、ツールバージョンに関する追跡（tracking）、解決に関する追跡、そして不適合報告システムの範囲の識別を含まなければならない(例えば、関連する申請者の数)。

c. 環境: ツールサービス履歴が収集されたツール運用環境の類似性と、提案されるプロジェクトで使用される類似性は、ツールサービス履歴発行を確立するために重要である。環境分析(environment analysis)は、ツール制限により課せられるツール利用上の制約を含まなければならない。

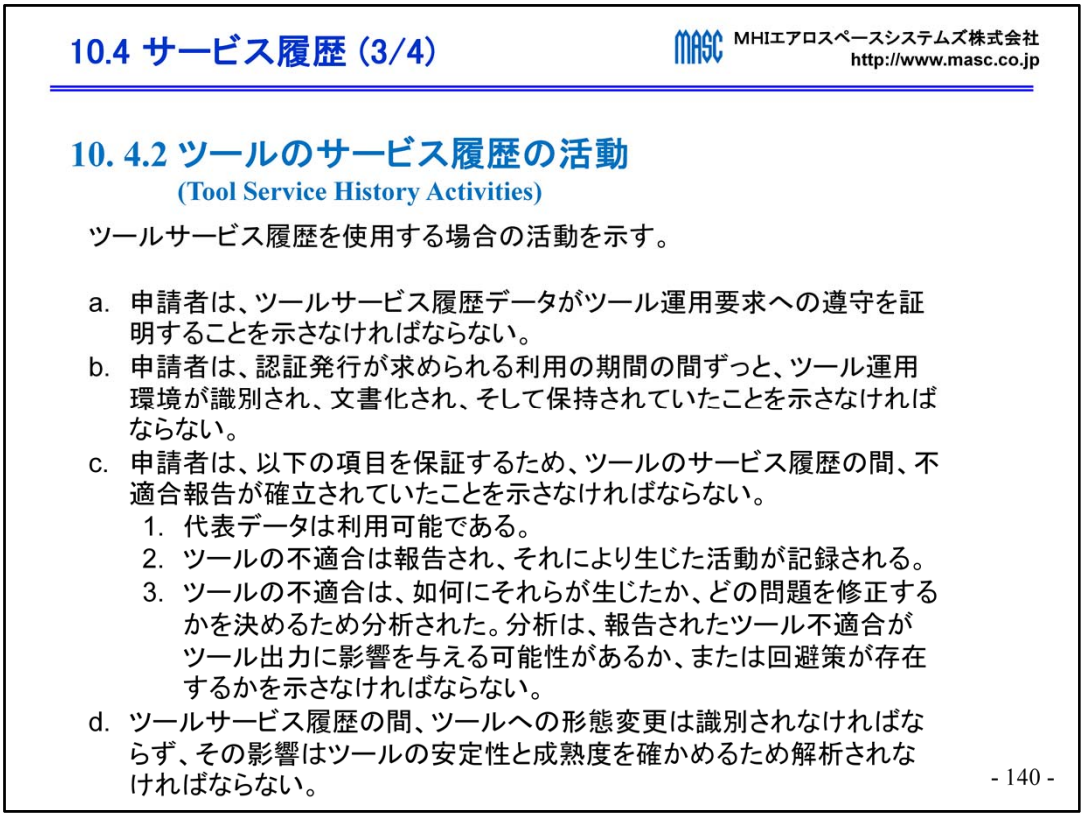
d. 運用(Operation): 運用モード(operating modes)やセッティング(settings)、ユーザーとの相互作用(interactions)、そして手順(procedures)は、提案されるツールアプリケーションのためツールサービス履歴の妥当性(relevance)を示すための、基本である。申請者側のツール使用経験及び(又は)トレーニングのレベルも、考慮されなければならない。運用分析(Operational analysis)は、申請者によって課されるツール使用の制約も、含まなければならない。

e. 安定性(Stability)と成熟度(maturity): ツールの変更履歴は、運用中(in-service)の安定性と成熟度を決定するため評価されなければならない。分析は、サービス履歴の存続期間(duration)がリセットされるかどうかを決定するため、ツールやツール運用環境上での変更の影響の評価を実施しなければならない。

f. アプリケーションサービス: ツールを使って開発されるアプリケーションのサービス履歴は、ツールの安定性と成

熟度の追加の実証を提供できなければならない。

《11.4.1》



【11.4.2】

《11.4.2》ツールサービス履歴の活動 (Tool Service History Activities)

ツールサービス履歴の使用のための活動には、以下がある。

a. 申請者は、ツールサービス履歴データがツール運用要求(Tool Operational Requirements)への遵守を証明することを示さなければならない。

b. 申請者は、認証発行が求められる利用の期間の間ずっと、ツール運用環境が識別され、文書化され、そして保持されていたこと示さなければならない。

c. 申請者は、以下の項目を保証するため、ツールのサービス履歴の間、不適合報告が確立されていたこと示さなければならない。
   1. 代表データ(Representative data)が利用可能である。
   2. ツールの不適合は報告され、結果とて起こる活動が記録される。
   3. ツールの不適合は、どのようにそれら生じて、どの問題が修正されたかを決定するために分析された。分析は、報告されたツール不適合がツール出力に影響を与える可能性があるか、または受け入れられる回避策が存在するかを示さなければならない。

d. ツールのサービス履歴の間ツールへの形態変更(configuration changes)は識別されなければならず、影響はツールの安定性と成熟度を確かめるため解析されなければならない。

e. ツール運用環境(tool operational environment)の解析は、ツールサービス履歴が適用できることを保証するため実施されなければならない。

f. ツールのサービス履歴は、ツールのサブセットの資格化を支援するために使われても良い。複数の機能を持つツールの資格化のためのガイダンスは、考慮されなければならない(11.1を参照)。

g. PSACやTQPは、意図されたツールの使用方法を記述しなければならず、また以下の項目を含まなければならない。
   1. サービス履歴データの要約(Summary)
   2. ツールのサービス履歴の利用のための理論的根拠と、どのようにそれがTQLと関連するか。
   3. ツールのサービス履歴環境の妥当性(relevance)の解析
   4. ツールサービス履歴の間の不適合報告の可用性(availability)
   5. ツールの安定性(stability)と成熟度(maturity)を評価するための、ツール変更履歴

《11.4.2》

10.4 サービス履歴 (4/4)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

10. 4.2 ツールのサービス履歴の活動 (続き)
(Tool Service History Activities)

e. ツール運用環境の解析は、ツールサービス履歴が適用できることを保証するため実施されなければならない。
f. ツールサービス履歴は、ツールのサブセットの資格化を支援するために使われても良い。複数の機能を持つツールの資格化のためのガイダンスは考慮されなければならない(11.1を参照)。
g. PSACやTQPには、意図されたツールの使用方法を記述しなければならず、以下の項目がなければならない。
   1. サービス履歴データの要約
   2. ツールのサービス履歴の利用のための理論的根拠と、それがTQLと関連する方法
   3. ツールのサービス履歴の環境の妥当性解析
   4. ツールサービス履歴の間の不適合報告の可用性
   5. ツールの安定性と成熟度を評価するための、ツール変更履歴

【11.4.2】

10.5 ツール資格化のための代替手法 (Alternative Methods for Tool Qualification)

申請者は、ツール資格化のため代替手法を使っても良い。可能性のある代替手法には、徹底的な入力テスト、形式手法、そしてデシミュラツールがあるが、それに限定されない。

代替手法を利用するための活動には以下がある。

a. ツール計画は、ツールライフサイクルプロセスと成果物の代替手法の申請を記述しなければならない。

b. 申請者は、以下の項目について、PSACやTQPで明確に述べ、認証機関から合意を得なければならない。
   (1) ソフトウェアライフサイクルプロセスへの提案される代替手法の影響
   (2) ソフトウェアライフサイクルデータへの提案される代替手法の影響
   (3) どのように本資料の目的が満たされるかを示す代替手法の利用のための理論的根拠

【11.5】

《11.5》ツール資格化のための代替手法 (Alternative Methods for Tool Qualification)

申請者は、ツール資格化のため代替手法を使うことを決定しても良い。可能性のある代替手法には、徹底的な入力テスト、形式手法、そしてデシミュラツール(dissimilar tools) (例えば、同じ運用要求を満たす、別々に開発される2つ以上のツール)があるが、それに限定されない。

代替手法は、全体的なソフトウェアライフサイクルプロセスの文脈(context)内で考えられなければならない。代替手法の認証発行(certification credit)を取得するための取り組みは、ソフトウェアライフサイクルにおける、ソフトウェアレベルと代替手法の影響力に依存する。代替手法を利用するための活動には以下がある。

a. ツール計画は、ツールライフサイクルプロセスと成果物の代替手法の申請を記述しなければならない。代替手法は、その時、手法の実装の正しさを証明しなければならない。

b. 申請者は、以下の項目について、PSACやTQPで明確に述べ、認証機関から合意を得なければならない。
   1. ソフトウェアライフサイクルプロセスへの提案される代替手法の影響
   2. ソフトウェアライフサイクルデータへの提案される代替手法の影響
   3. どのように本資料の目的が満たされるかを示す代替手法の利用のための理論的根拠(記述(description)、正当化(justification)、実証(substantiation)など)

《11.5》

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

各TQLで要求されるツール資格データ

A-1. 要求されるツール資格データ
A-2. TQLによるツール資格データ数の比較

A-1. 要求されるツール資格データ (1/3)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

1. ツール資格連絡プロセスと他のインテグラルプロセスにおけるデータ

No	名称	TQL				
		1	2	3	4	5
1	PSAC内のツール固有情報(Tool-Specific Information in PSAC)	○	○	○	○	○
2	ツール資格計画(Tool Qualification Plan)	○	○	○	○	●
3	ツール開発計画(Tool Development Plan)	○	○	○	○	
4	ツール検証計画(Tool Verification Plan)	○	○	○	○	
5	ツール形態管理計画(Tool Configuration Management Plan)	○	○	○	○	
6	ツール品質保証計画(Tool Quality Assurance Plan)	○	○	○	○	
7	ツール要求標準(Tool Requirements Standards)	○	○	○		
8	ツール設計標準(Tool Design Standards)	○	○	○		
9	ツールコード標準(Tool Code Standards)	○	○	○		
10	ツールライフサイクル環境形態索引 (Tool Life Cycle Environment Configuration Index)	○	○	○	○	
11	ツール形態索引(Tool Configuration Index)	○	○	○	○	●
12	ツール不適合報告(Tool Problem Reports)	○	○	○	○	
13	ツール形態管理記録(Tool Configuration Management Records)	○	○	○	○	○
14	ツール品質保証記録(Tool Quality Assurance Records)	○	○	○	○	●
15	ツール完了報告(Tool Accomplishment Summary)	○	○	○	○	●
16	ソフトウェア完了報告内のツール特有情報 (Tool-Specific Information in Software Accomplishment Summary)	○	○	○	○	○
17	ソフトウェアライフサイクル環境形態索引内のツール特有情報 (Tool-Specific Information in Software Life Cycle Environment Configuration Index)	○	○	○	○	○

●:ソフトウェアライフサイクルプロセスの成果物にまとめられても良いもの

- 144 -

各TQLで要求されるツール資格データ(Tool Qualification Data)を示す。
○がついている項目が、そのTQLで開発しなければならないツール資格データである。

TQL-5の場合、成果物の一部(TQP, TCI, ツール品質保証記録, TAS)はソフトウェアライフサイクルプロセスの成果物にまとめられても良い。
その項目を●で示した。

A-1. 要求されるツール資格データ (2/3)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

2. ツール開発プロセスと対応する検証活動の間に作られたツール資格データ

No	名称	TQL				
		1	2	3	4	5
1	ツール要求(Tool Requirements)	○	○	○	○	
2	ツール設計記述(Tool Design Description)	○	○	○	○	
3	ツールソースコード(Tool Source Code)	○	○	○		
4	ツール実行可能オブジェクトコード(Tool Executable Object Code)	○	○	○	○	○
5	ツール検証ケース・手順(Tool Verification Cases and Procedures)	○	○	○	○	
6	ツール検証結果(Tool Verification Results)	○	○	○	○	
7	トレースデータ(Trace Data)	○	○	○	○	

A-1. 要求されるツール資格データ (3/3)

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

3. ツール運用要求プロセスとツール運用統合プロセス、および対応する検証/妥当性確認活動の間に作られたツール資格データ

No	名称	TQL				
		1	2	3	4	5
1	ツール運用要求(Tool Operational Requirements)	○	○	○	○	○
2	ツールインストール報告(Tool Installation Report)	○	○	○	○	○
3	ツール運用要求検証/妥当性確認ケース・手順 (Tool Operational Verification and Validation Cases and Procedures)	○	○	○	○	○
4	ツール運用要求検証/妥当性確認結果 (Tool Operational Verification and Validation Results)	○	○	○	○	○

A-2. TQLによるツール資格データ数の比較

MHIエアロスペースシステムズ株式会社
http://www.masc.co.jp

各TQLで要求されるツール資格データ(Tool Qualification Data)の数を以下に示す。

	ツール資格レベル (Tool Qualification Level)				
	TQL-1	TQL-2	TQL-3	TQL-4	TQL-5
要求されるツール資格データの数	28	28	28	24	12(9)

* カッコ内の数字は、ツール資格データをソフトウェアライフサイクルプロセスの成果物にまとめる場合の成果物の数である(TQL-5の場合のみ)。

参考 TQLに要求されるObjectivesの数

	ツール資格レベル (Tool Qualification Level)				
	TQL-1	TQL-2	TQL-3	TQL-4	TQL-5
要求されるObjectivesの数	76(35)	74(22)	70(5)	38(2)	14(2)

()内は独立した組織が実行

【参考文献】

◇ RTCA/DO-178C

Software Considerations in Airborne Systems and Equipment Certification

◇ RTCA/DO-330

Software Tool Qualification Considerations